Ethernet Fundamentals Overview: Part 2 (Mod 6)

Cabrillo College

CIS 81 and CST 311

Rick Graziani

Cabrillo College

Spring 2006

Ethernet Fundamentals

Part 1

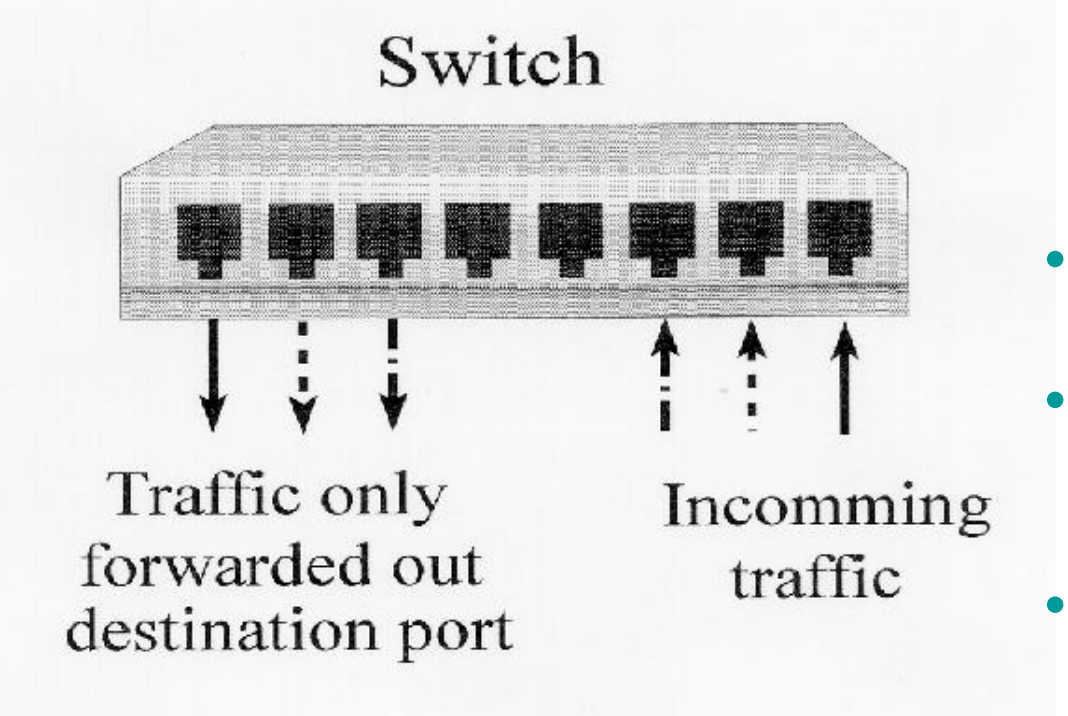
- Introduction to Ethernet

Part 2

- Layer 2 and Ethernet Switches
- Cables, Duplex, and Troubleshooting
- Ethernet and the OSI Model – more detail
- Ethernet frames – more detail

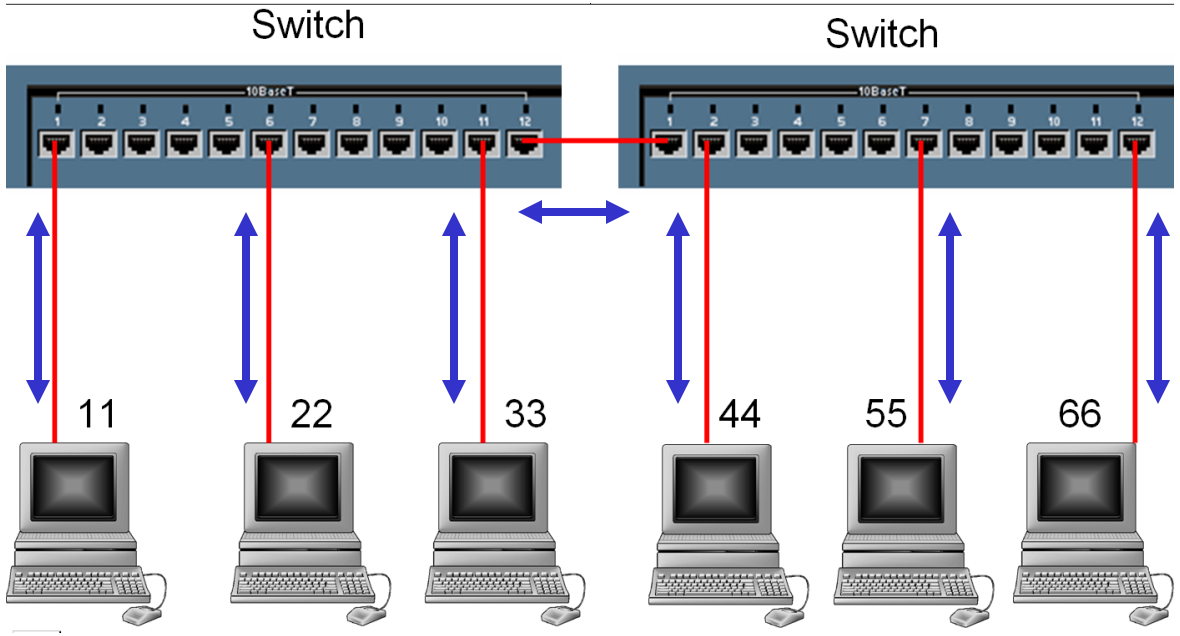
Layer 2 and Ethernet Switches

Sending and receiving Ethernet frames via a switch



- Layer 2 device (also includes layer 1) which examines and bases its decisions on the information in layer 2 frames
- Switch ports typically operate in **full-duplex**.
- Multiple devices on the switch can communicate at a time, otherwise collisions occur.
- 10/100 Mbps ports are the most common.
- 1000 Mbps also are also common, usually connecting to another switch or router.

Full-duplex (More in next section)



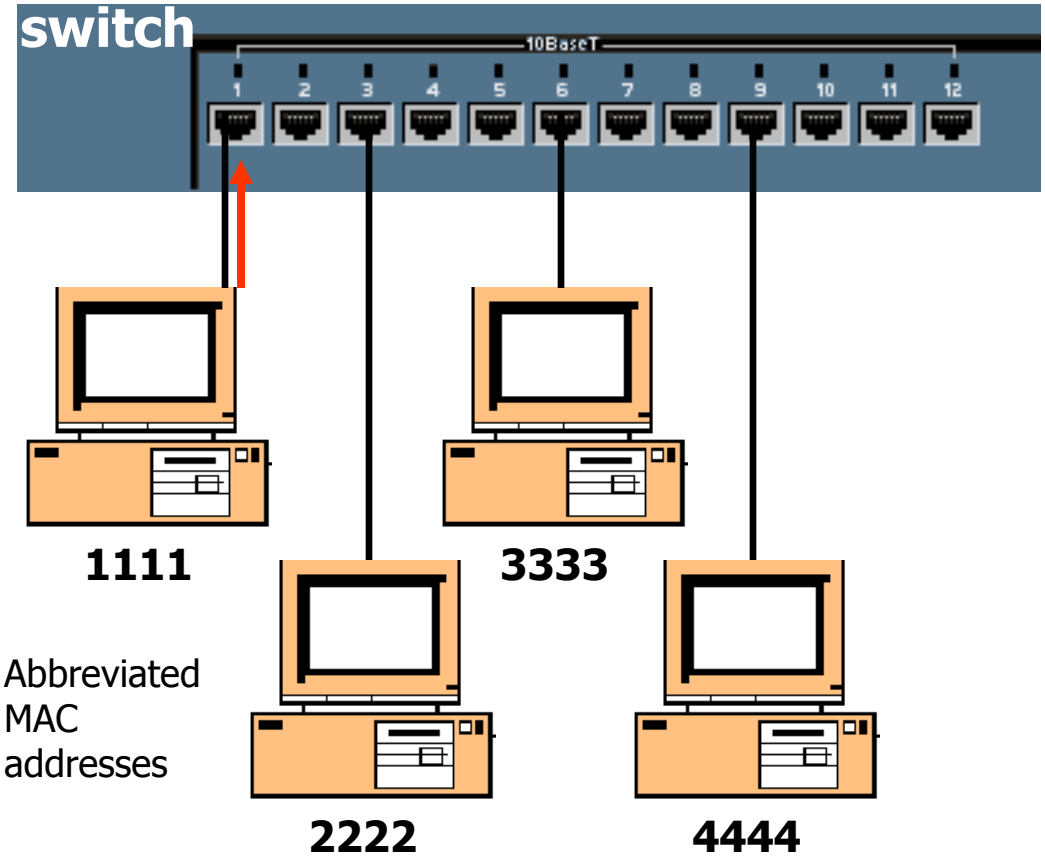
- **Full-duplex** is allows simultaneous communication between a pair of stations or devices.
- Full-duplex allows devices to send and receive at the same time.
- Both ends of the link must be in full-duplex mode.
- In full-duplex, the station ignores any collision detect signals that come from the transceiver.
- If a hub is connected to a switch, the switch port must be in half-duplex.
- The collision domain will end at the switch port.

Learning Switches: Learns Source MAC Address

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	3333	**1111**				



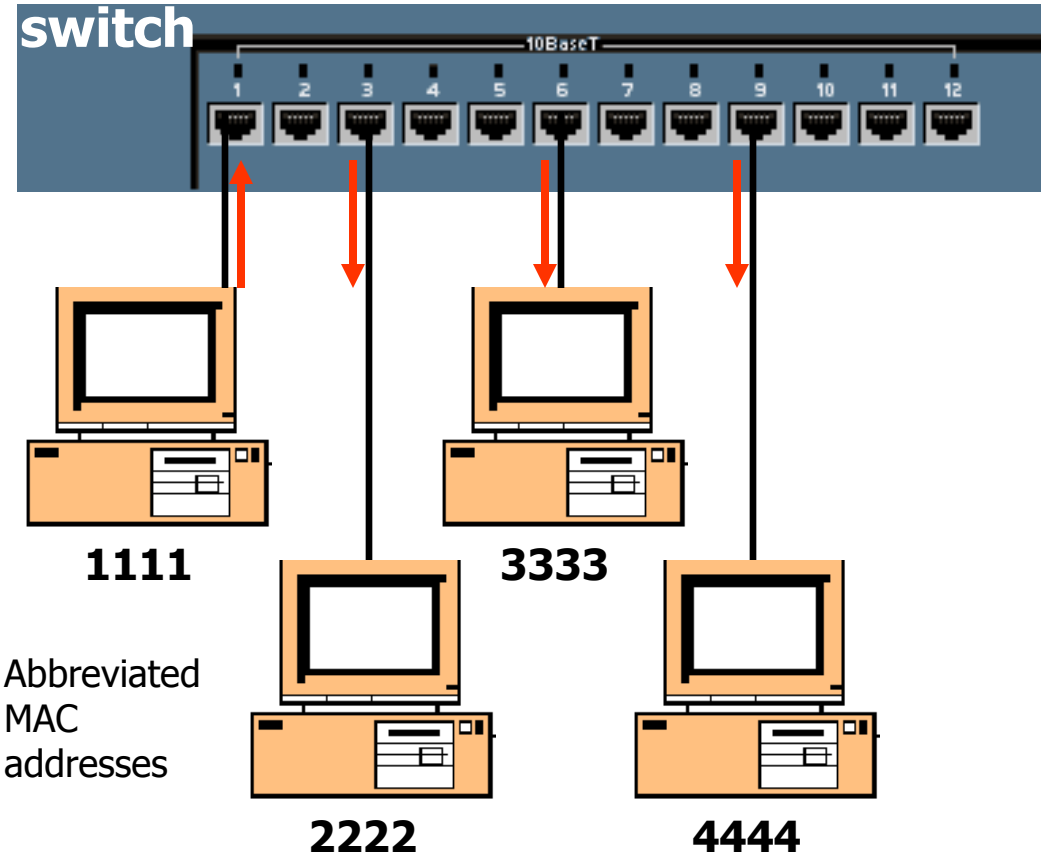
- Switches are also known as **learning bridges** or **learning switches**.
- A switch has a **source address table** (or **MAC Address Table**) in cache (RAM) where it stores a source MAC address after it learns about them.
- How does it learn source MAC addresses?
- Whenever a frame enters a switch, it will first see if the **Source Address** (1111) is in it's table.
  - If it is, it **resets the timer** (more in a moment).
  - If it is NOT in the table it **adds** it, with the port number.

Destination MAC Address: Filter or Flood

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	3333	1111				



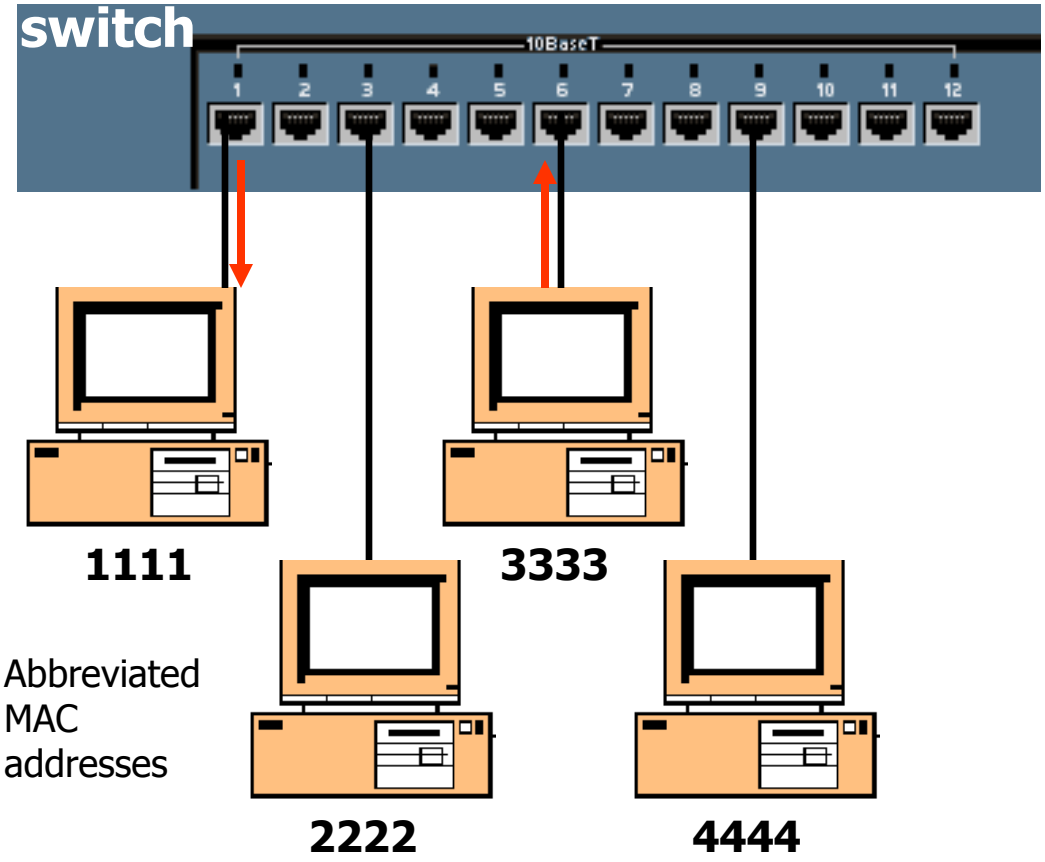
- Next, the switch examines the source address table for the **Destination MAC address**.
- If it finds a match, it **filters** the frame by only sending it out that port.
- If there is **not** a match if **floods** it out all ports.
- In this scenario, the switch will **flood** the frame out all other ports, because the **Destination Address** is **not** in the source address table.

Learning Switches: Learns, Filter or Flood

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	1111	3333				



- Most communications involve some sort of **client-server relationship** or exchange of information. (You will understand this more as you learn about TCP/IP.)
- Now 3333 sends data back to 1111.
- The switch sees if it has the **Source Address** stored.
- It does **NOT** so it adds it. (This will help next time 1111 sends to 3333.)
- Next, it checks the **Destination Address** and in our case it can **filter** the frame, by sending it only out port 1.

Destination Address in table, Filter

Source Address Table

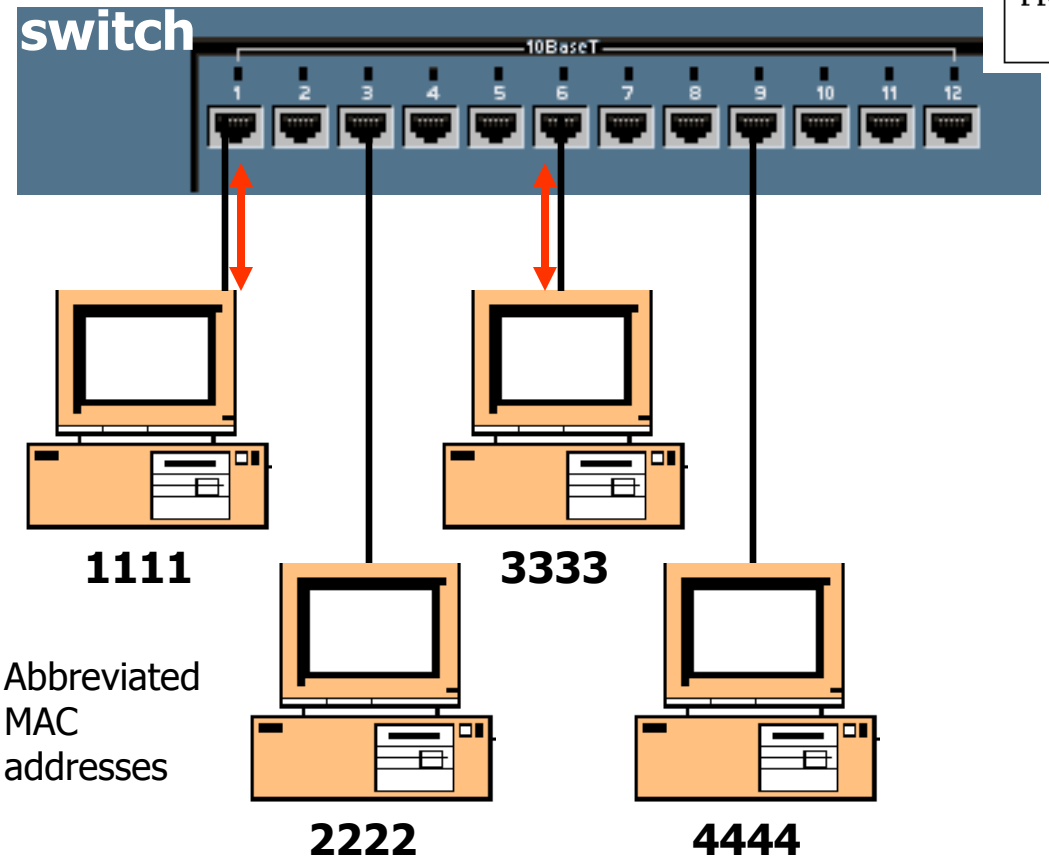
Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 1111

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 3333



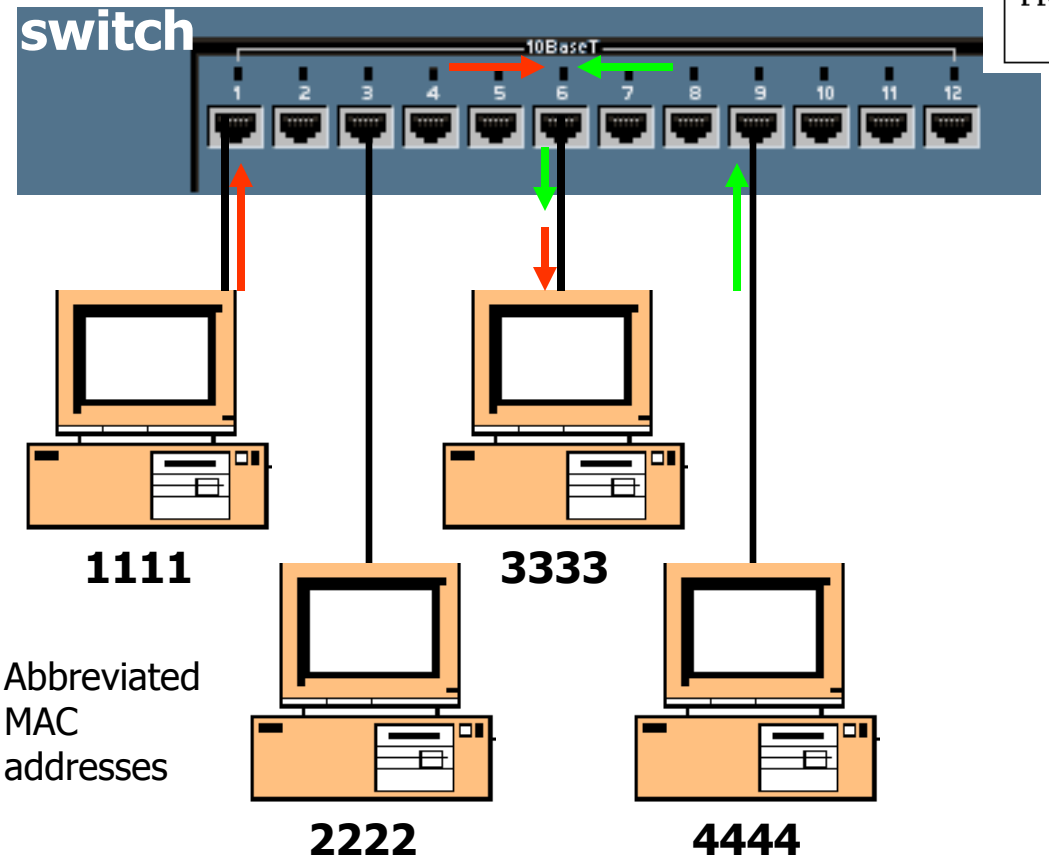
- Now, because both MAC addresses are in the switch's table, any information exchanged between 1111 and 3333 can be sent (**filtered**) out the appropriate port.

- **What happens when two devices send to same destination?**
- **What if this was a hub?**
- **Where is (are) the collision domain(s) in this example?**

No Collisions in Switch, Buffering

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		



Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **1111**

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **4444**

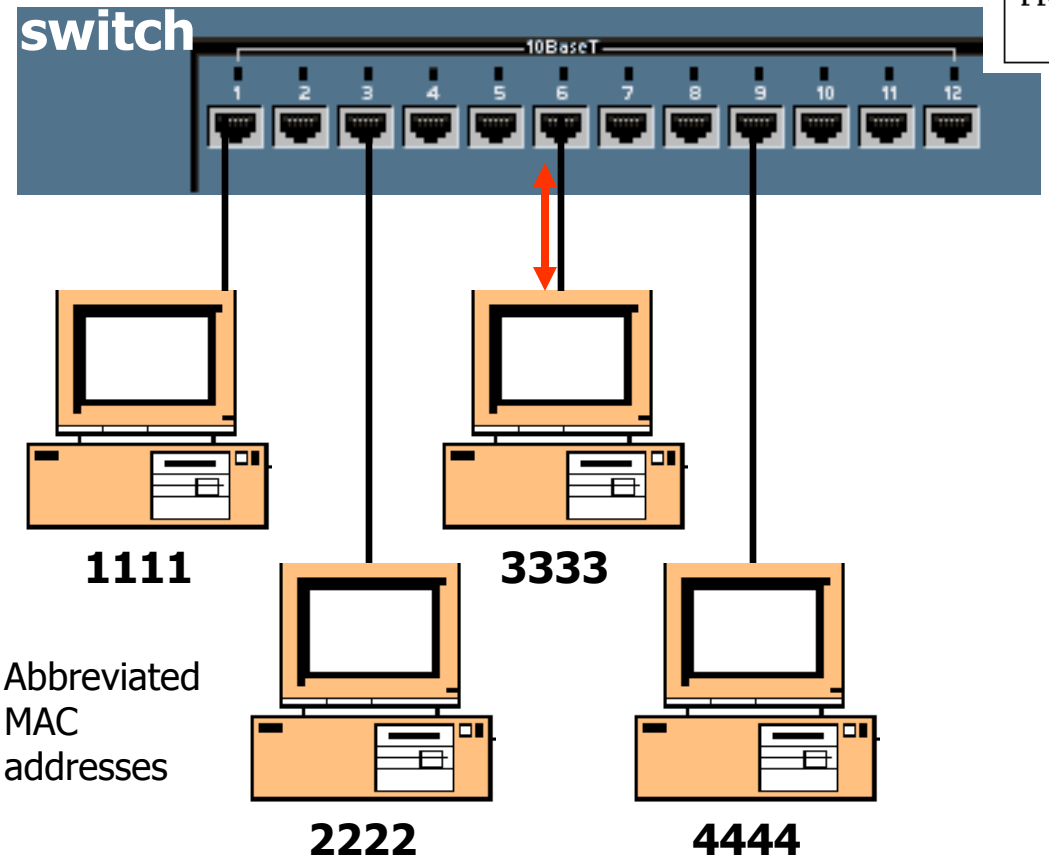
- Unlike a hub, a **collision does NOT occur**, which would cause the two PCs to have to retransmit the frames.
- Collision domains end at the switch
- Instead the switch **buffers** the frames and sends them out port #6 one at a time.
- The sending PCs have no idea that their was another PC wanting to send to the same destination.

Full Duplex – No collisions

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		

No Collision Domains



Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **1111**

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **4444**

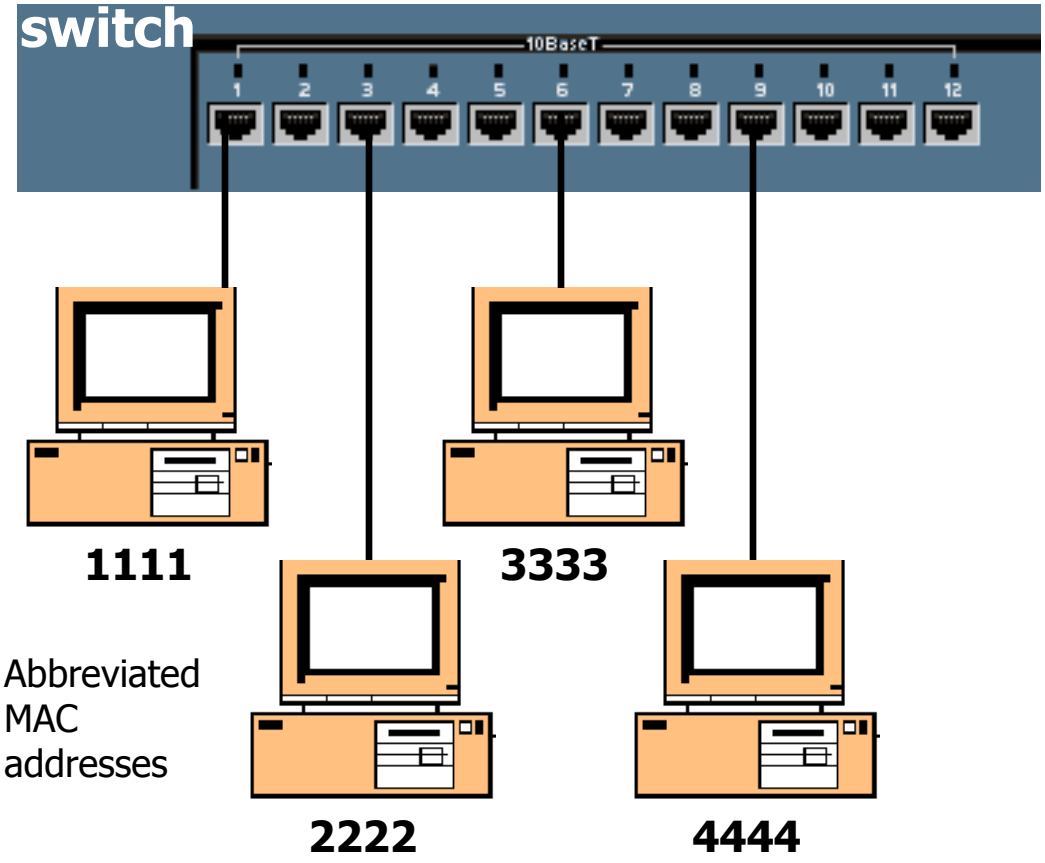
- When there is only one device on a switch port, the collision domain is only between the PC and the switch, which is non-existent with full-duplex.
- With a **full-duplex** PC and switch port, there will be no collision, since the devices and the medium can send and receive at the same time.

Other Information

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC



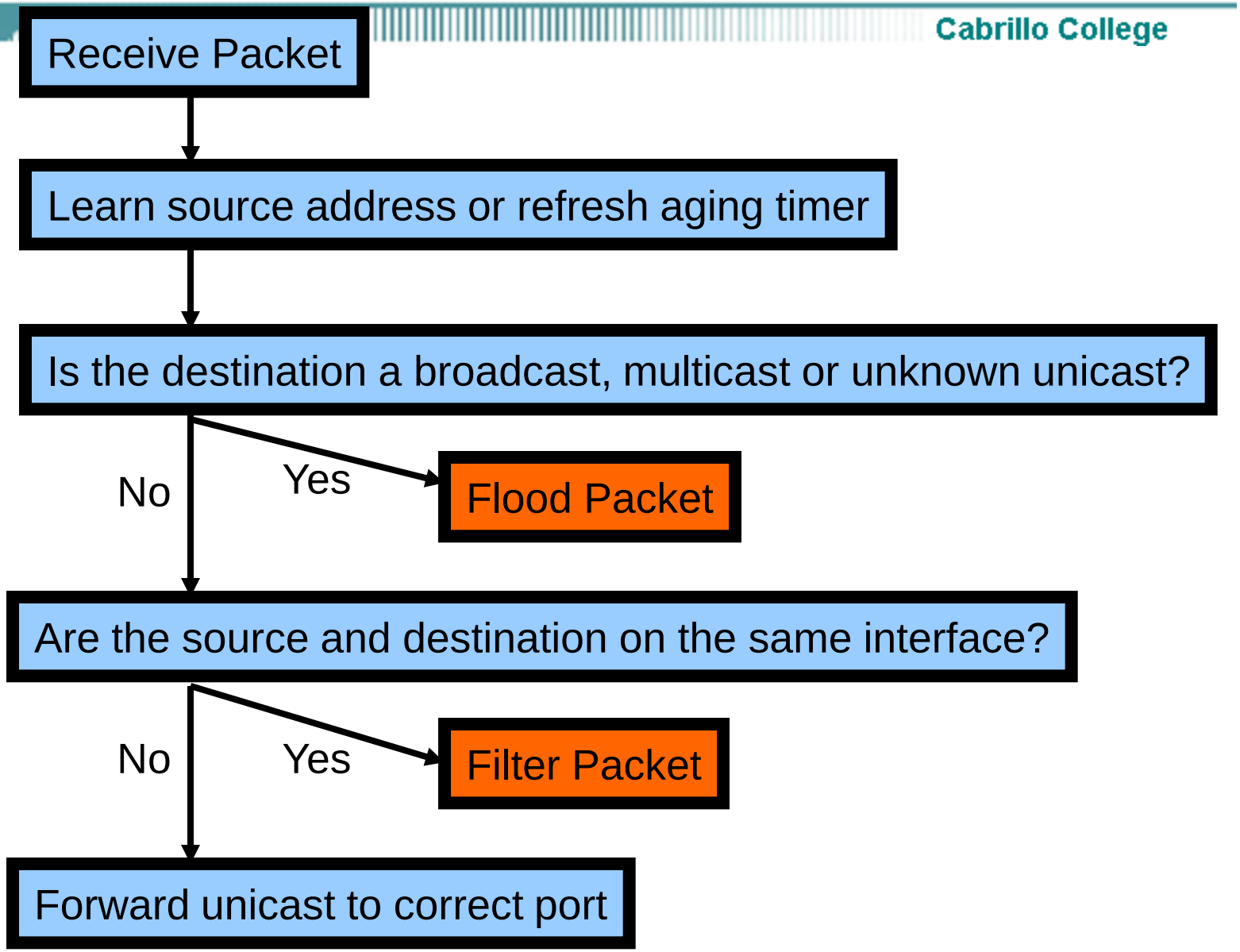
- How long are addresses kept in the Source Address Table?
  - 5 minutes is common on most vendor switches.
- How do computers know the Destination MAC address?
    - ARP Caches and ARP Requests (later)
- How many addresses can be kept in the table?
  - Depends on the size of the cache, but 1,024 addresses is common.
- What about Layer 2 broadcasts?
  - Layer 2 broadcasts (DA = all 1's) is flooded out all ports.

Side Note - Transparent Bridging

- Transparent bridging (normal switching process) is defined in IEEE 802.1D describing the five bridging processes of:
  - learning
  - flooding filtering
  - forwarding
  - aging

- These will be discussed further in STP (Spanning Tree Protocol), which is also part if IEEE 802.1D.

Transparent Bridge Process - Jeff Doyle



Switch Process – Another Look

For every frame that enters a switch…

- Learning Stage (Building/Updating of SAT/MAC table)
  - Examines **Source MAC Address**:
    - If **Source MAC Address** is in the SAT/MAC table, update 5 minute timer
    - If **Source MAC Address** is NOT in the SAT/MAC table, add Source MAC Address and incoming port number to SAT/MAC table
- Forwarding Stage (Flood or Filter)
  - Examines **Destination MAC Address**:
    - If **Destination MAC Address** is in the SAT/MAC table, forward the frame only out that port (**Filter**), unless it is the outgoing port is the same as the incoming port (checks Source MAC Address)
    - If **Destination MAC Address** is NOT in the SAT/MAC table, forward the frame only out all ports except incoming port (**Flood**)

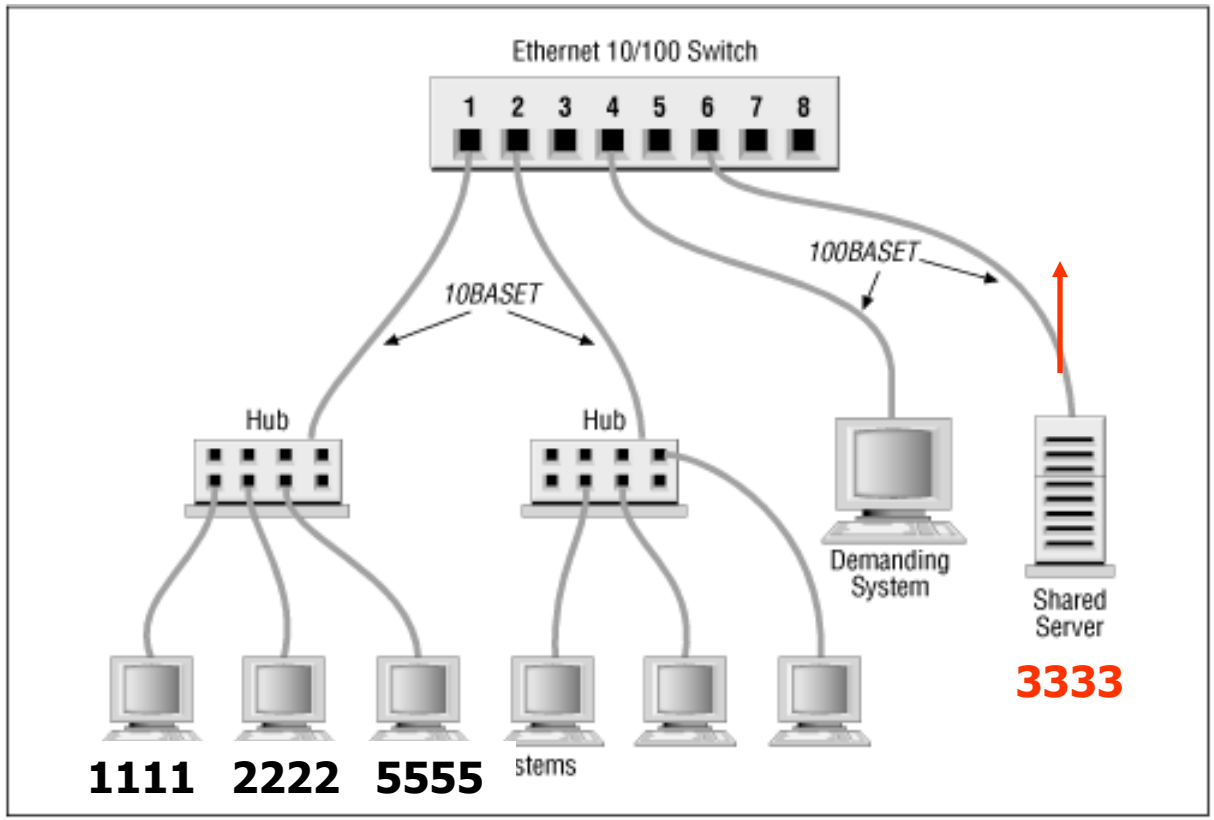
What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**	6	3333
1	**2222**	**1**	**5555**

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 **3333**



- Notice the Source Address Table has multiple entries for port #1.

What happens here?

Source Address Table

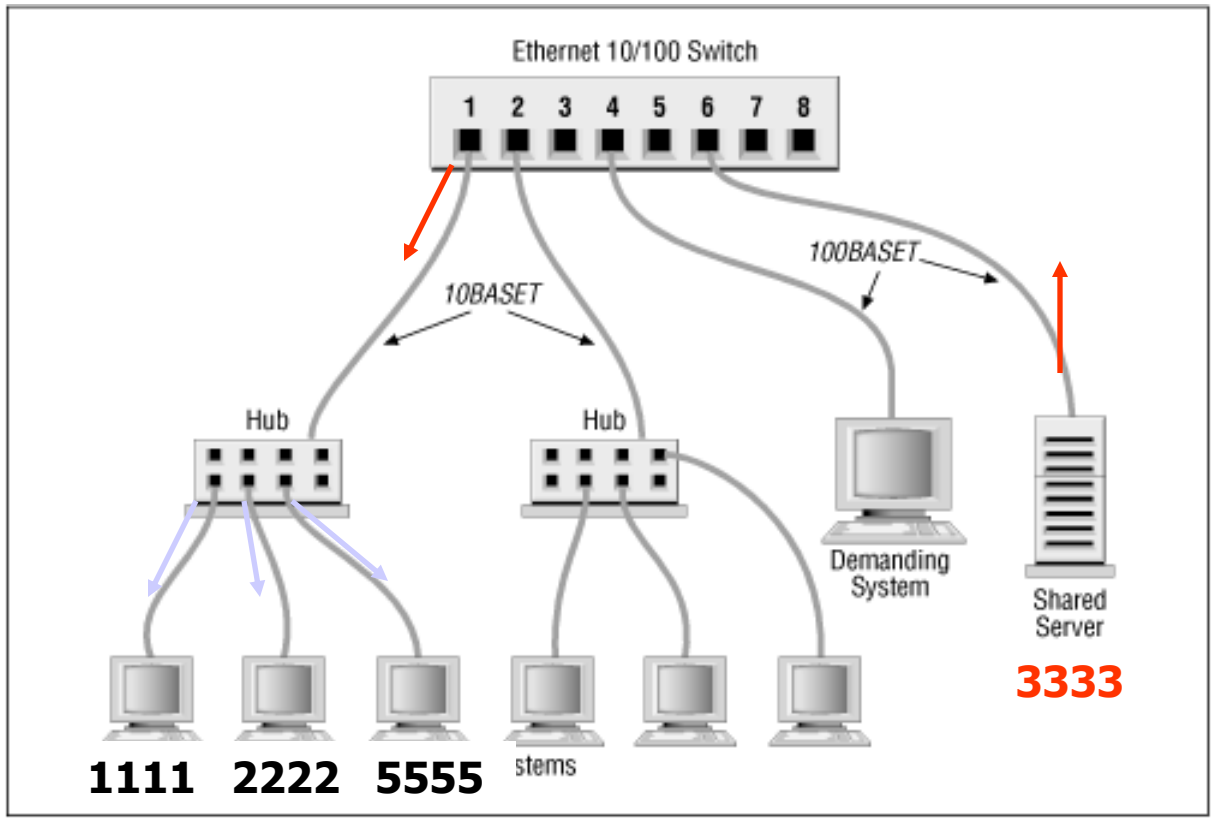
Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**	6	3333
1	**2222**	**1**	**5555**

Filter

Reset timer

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 **3333**



- The switch **resets the 5 minute timer** on the source port entry.
- The **switch filters** the frame out port #1.
- But the hub is only a layer 1 device, so a **hub floods** it out all ports.
- Where is the collision domain?

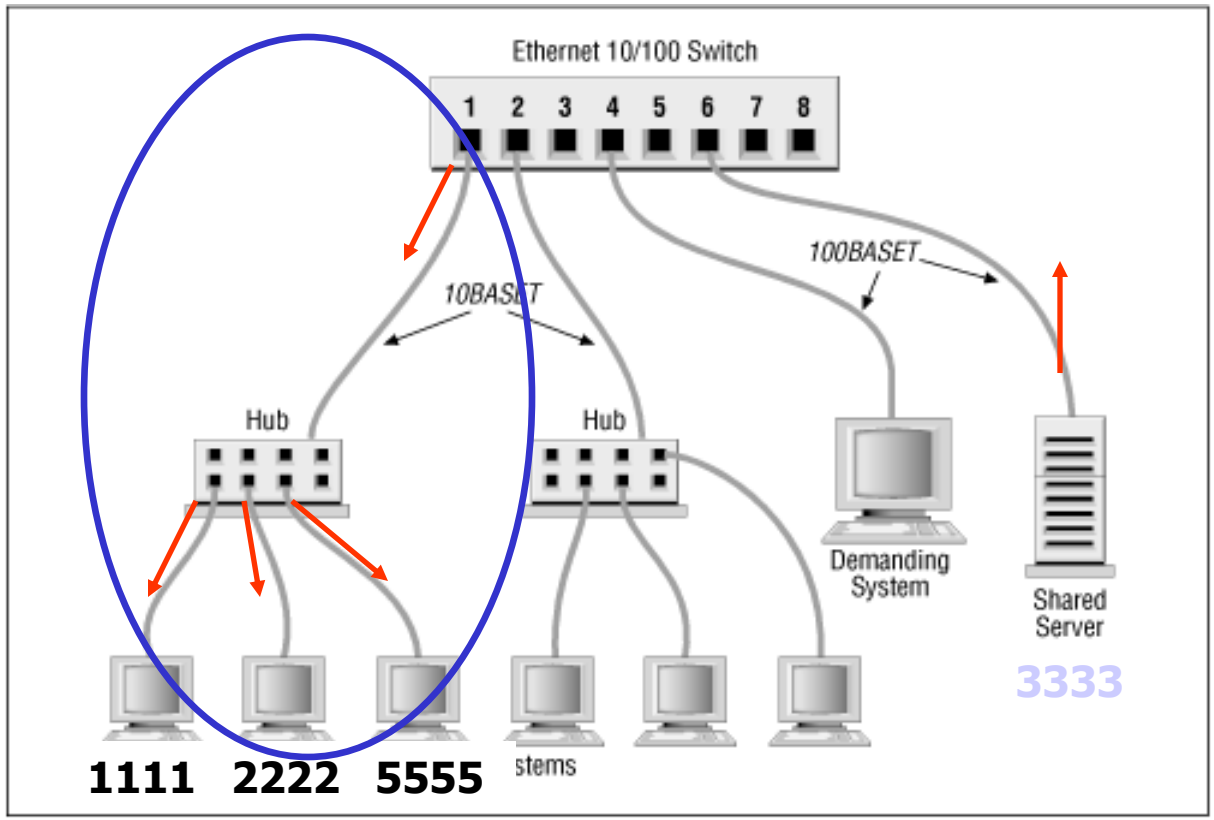
What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	**1111**	6	3333
1	**2222**	**1**	**5555**

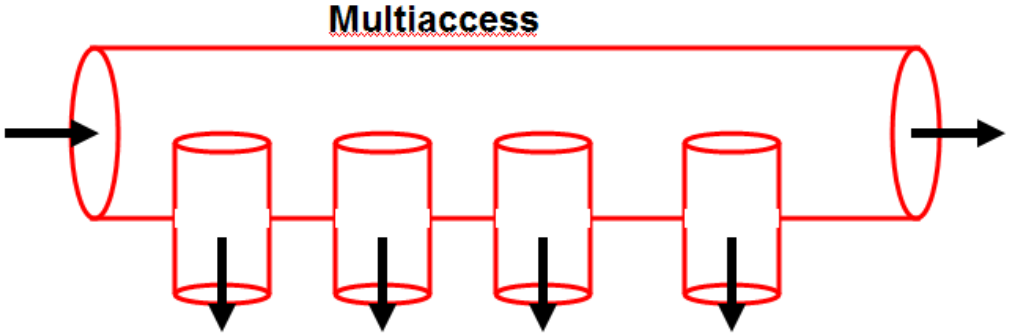
Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 **3333**



Collision Domain

Ethernet LANs are multiaccess networks



router

switch

switch

switch

hub

hub

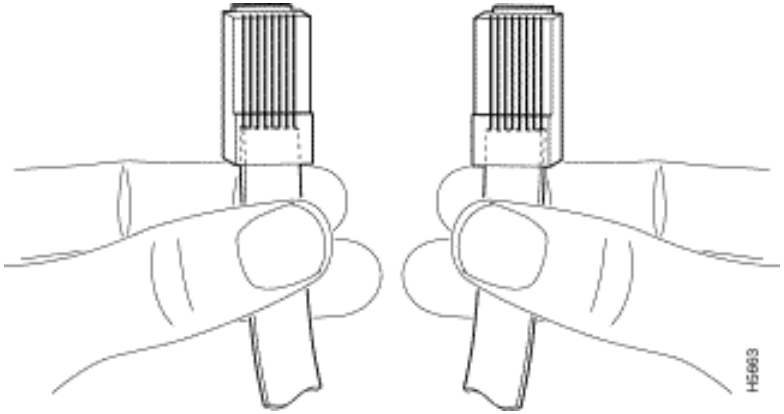
switch

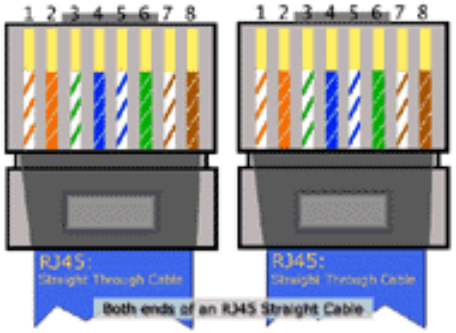
switch

switch

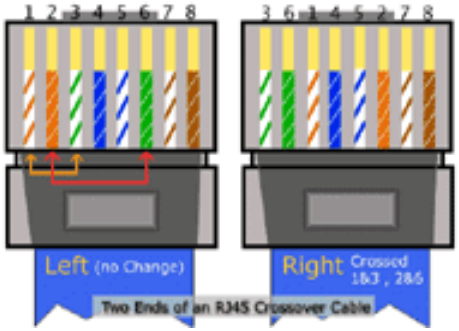
Cables, Duplex, Troubleshooting

Unshielded Twisted Pair (UTP)

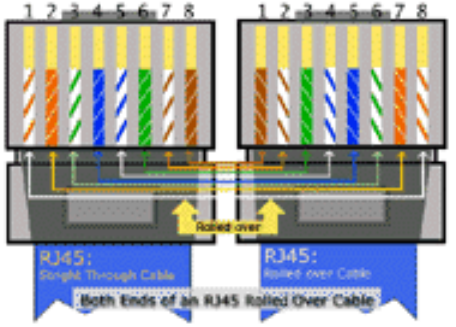




Straight-through



Cross-over

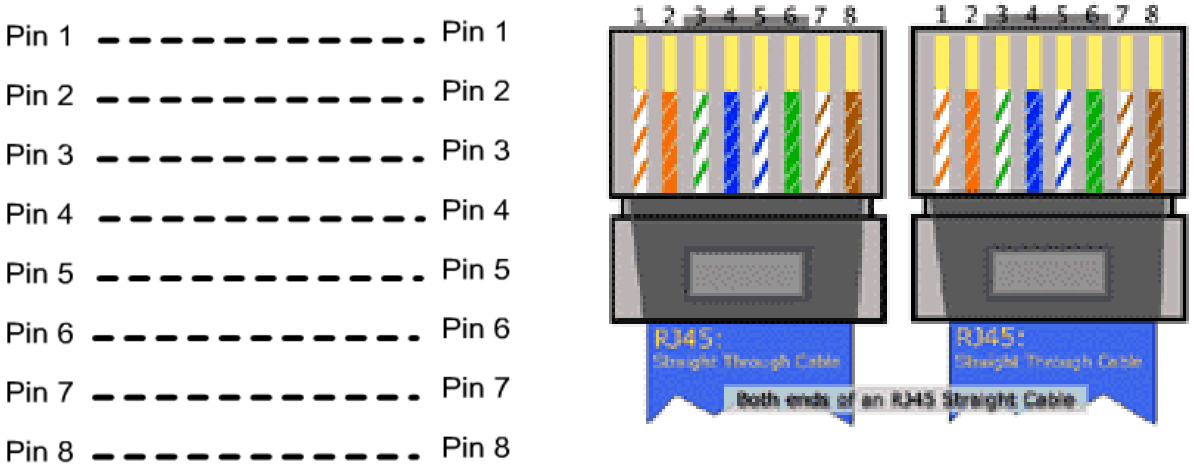


Rollover

www.cisco.com/warp/ public/701/14.html

UTP Straight-through Cable

Hub or Switch **Host or Router**

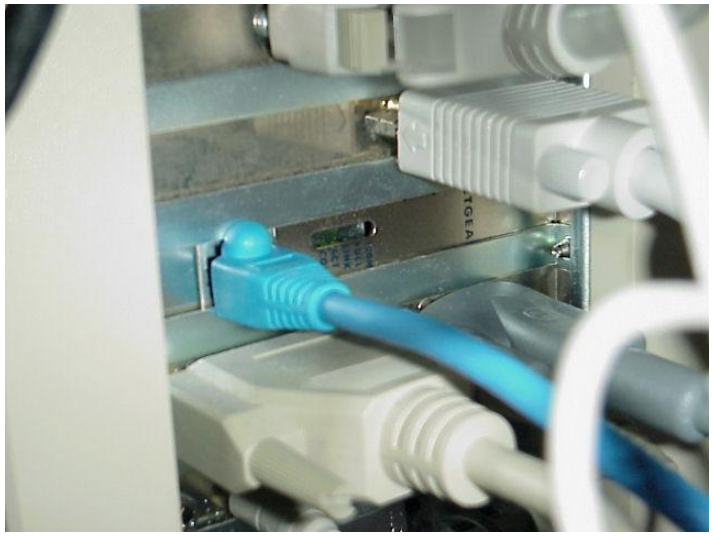


- The cable that connects from the switch port to the computer NIC port is called a straight-through cable.
- Connects unlike devices.

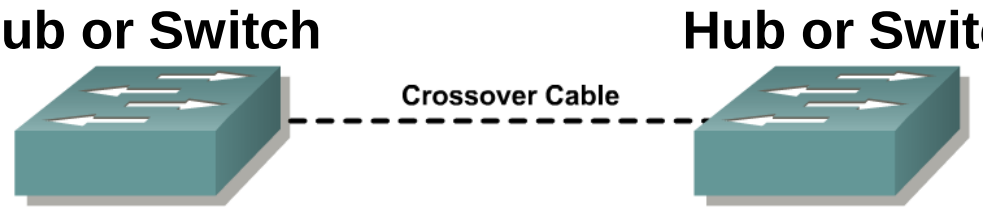
UTP Straight-through Cable

Hub or Switch

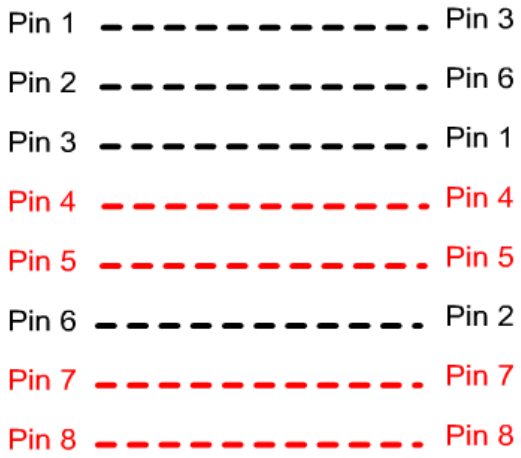
Host or Router

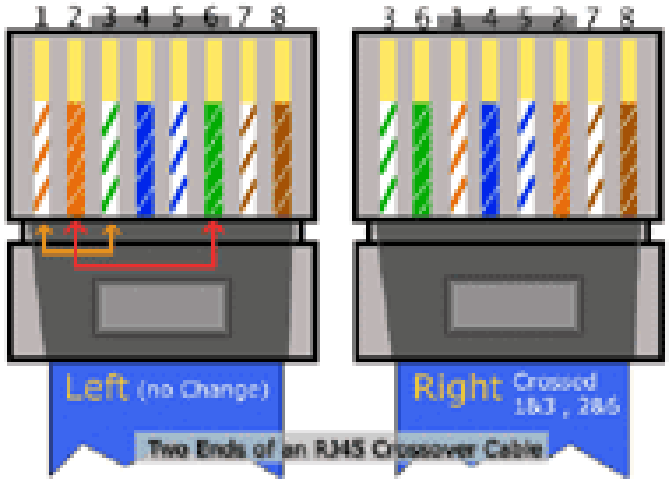


UTP Cross-over Cable



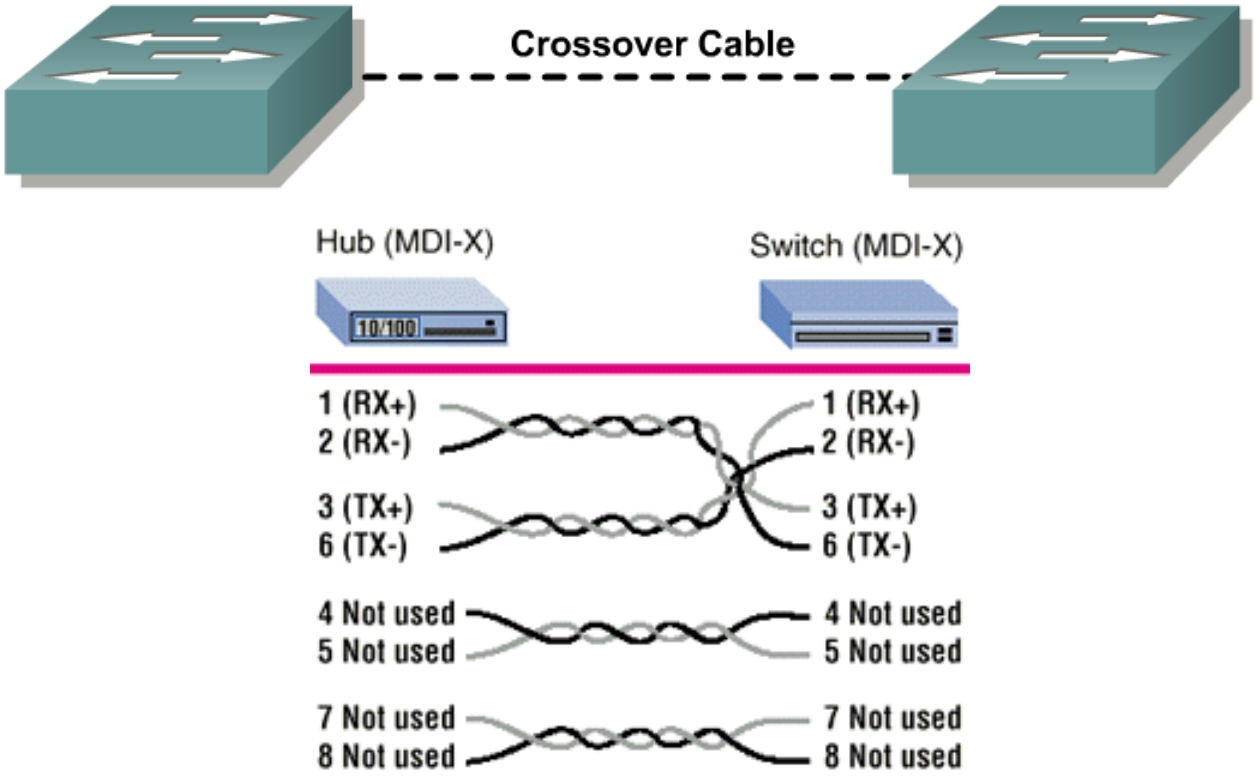
An Ethernet (10BASE-T and 100BASE-TX) cross-connect cable has only four active wires 1, 2, 3, and 6



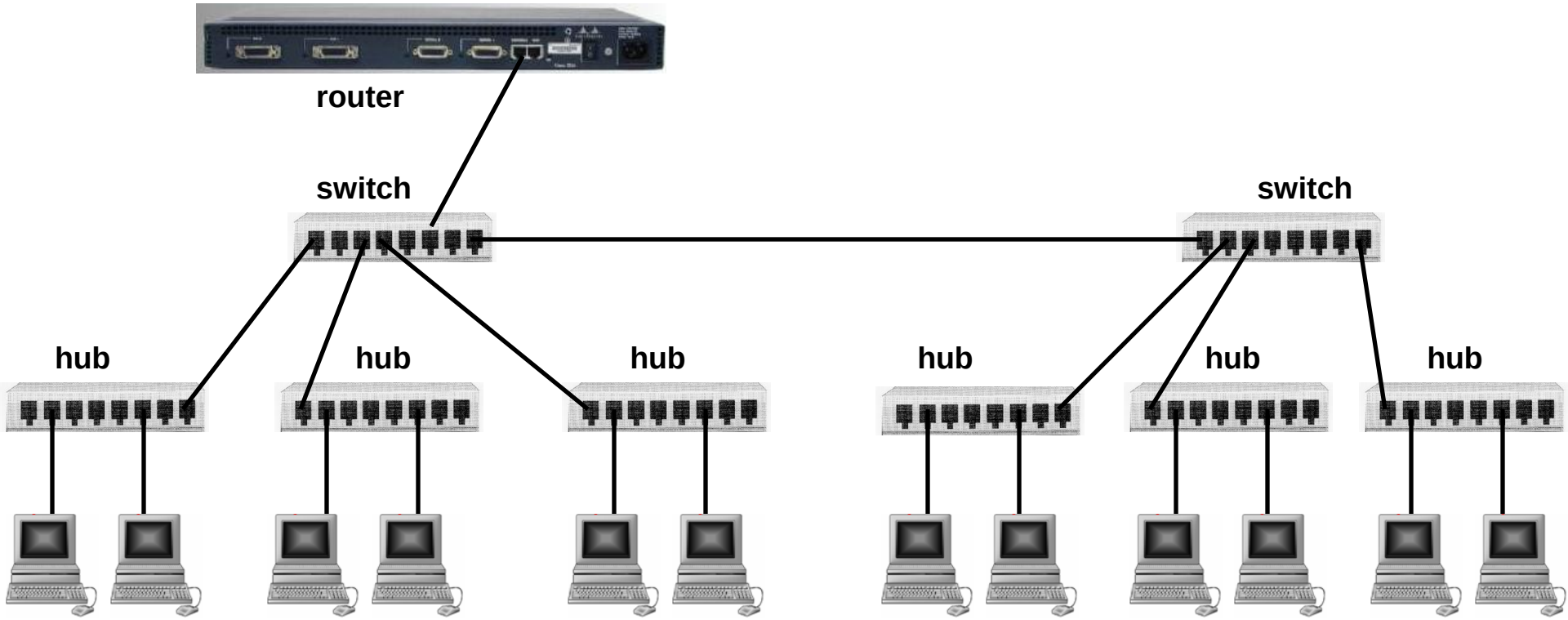


- The cable that connects from one switch port to another switch port is called a crossover cable.
- Connects like devices.

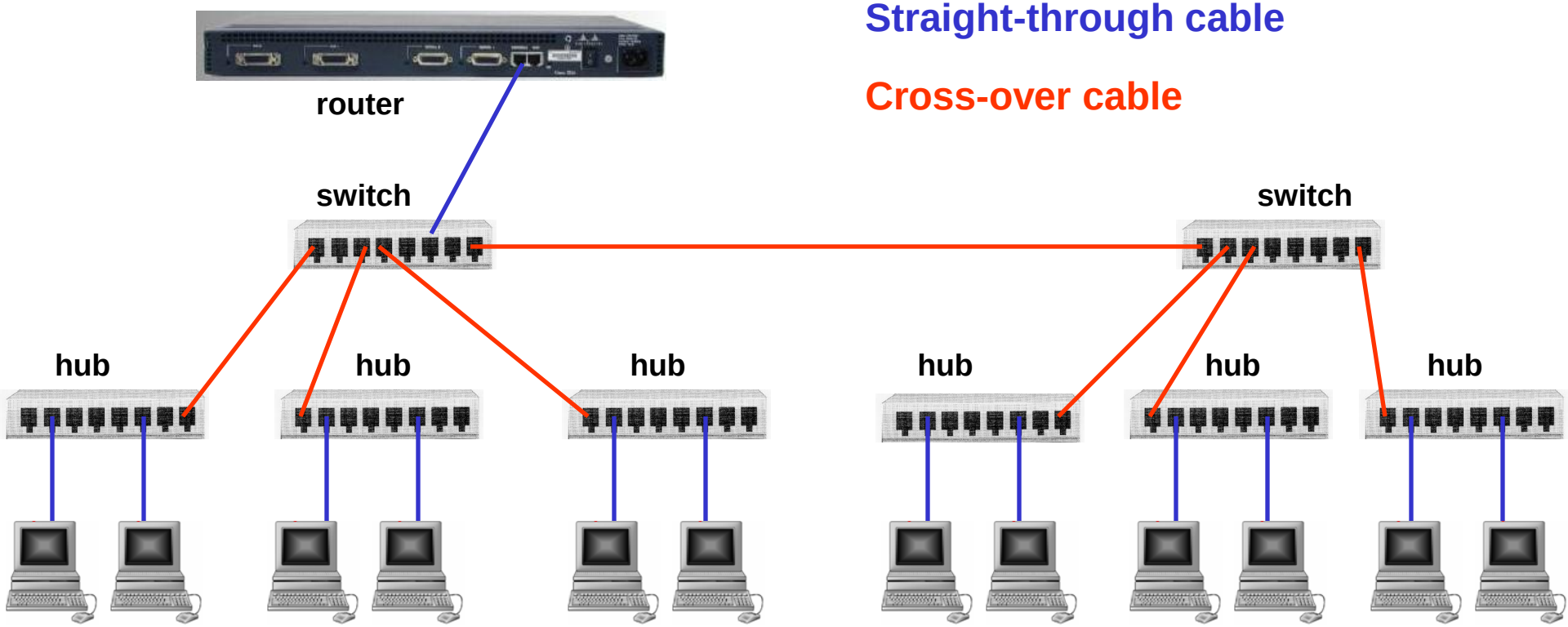
UTP Cross-over Cable



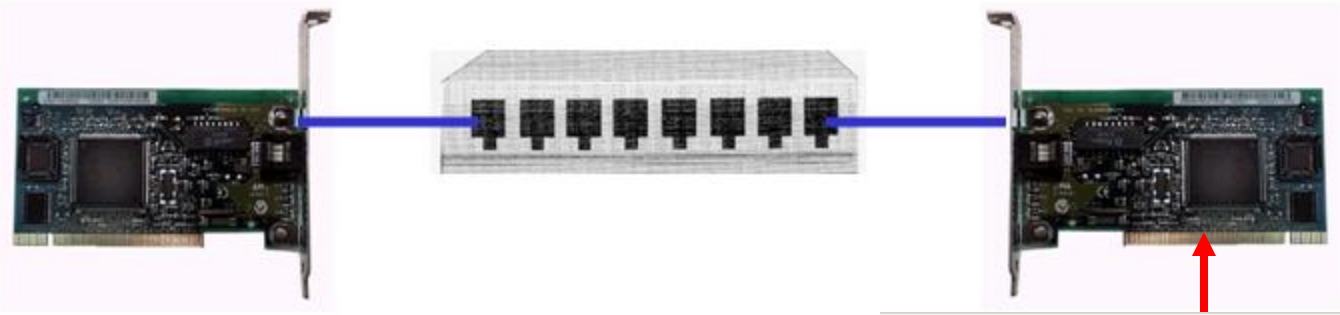
Cabling – Show the straight-through and cross-over cables



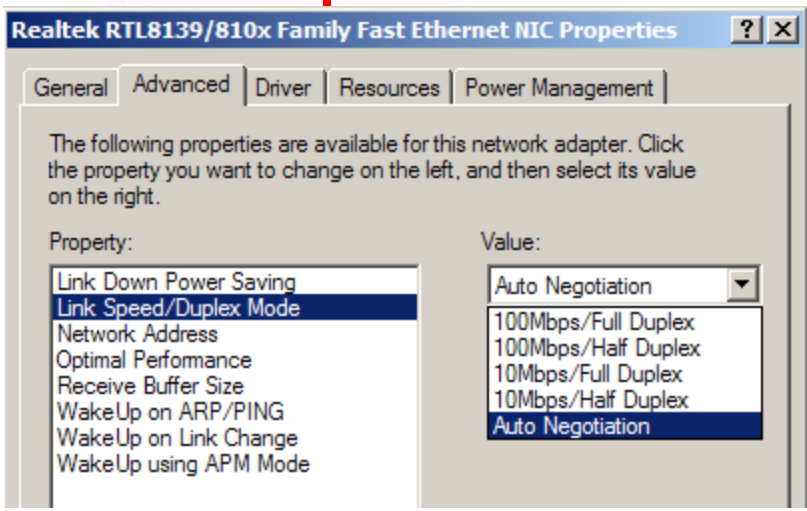
Cabling – Show the straight-through and cross-over cables



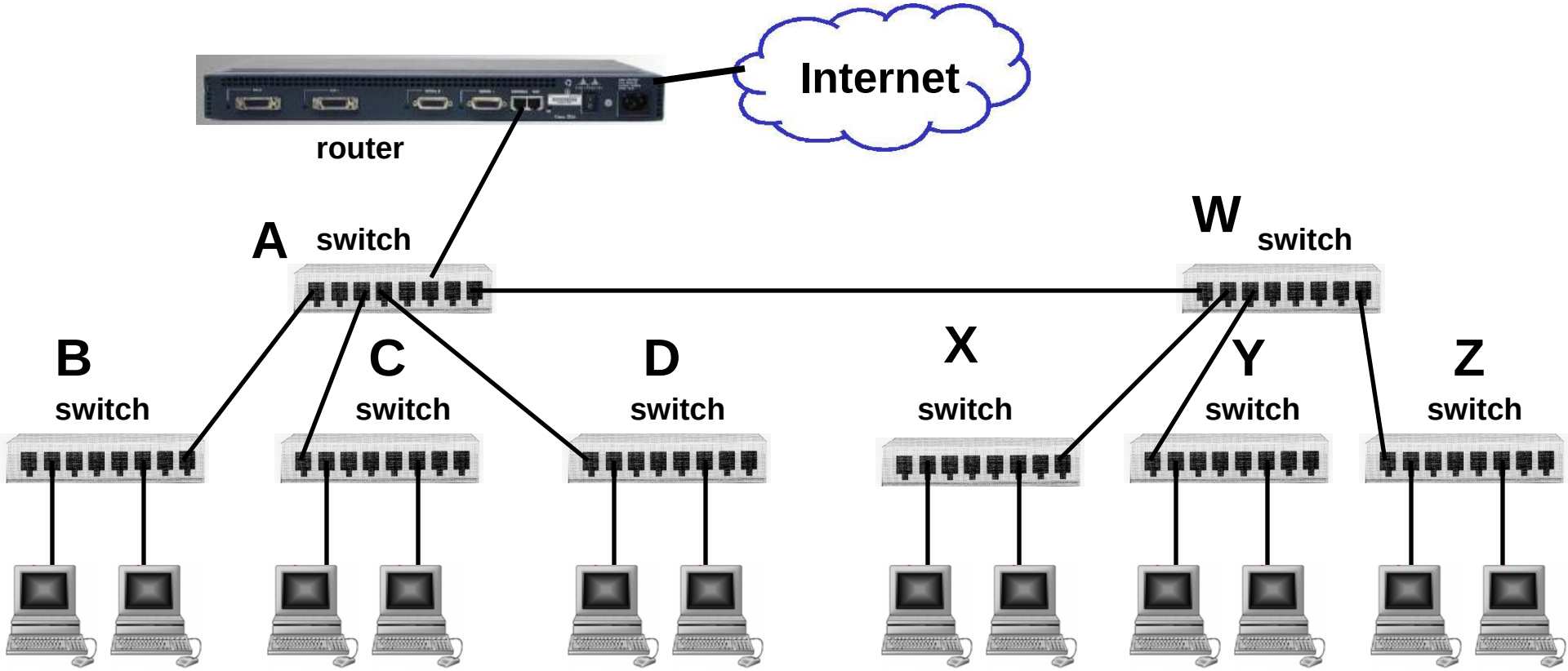
Configuring Speed and Duplex



- Negotiation between NIC and switch port.
  - Duplex: Full-duplex or Half-duplex
  - Speed: 10/100/1000 Mbps
  - Autonegotiation
    - Both sides of a link should have auto-negotiation on, or both sides should have it off.

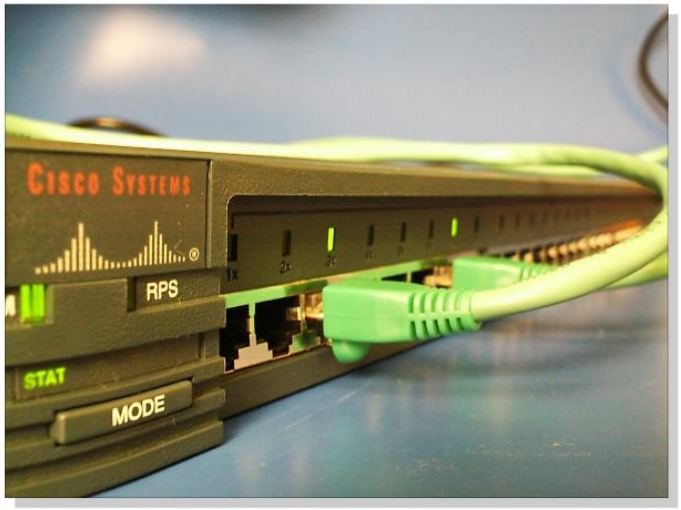


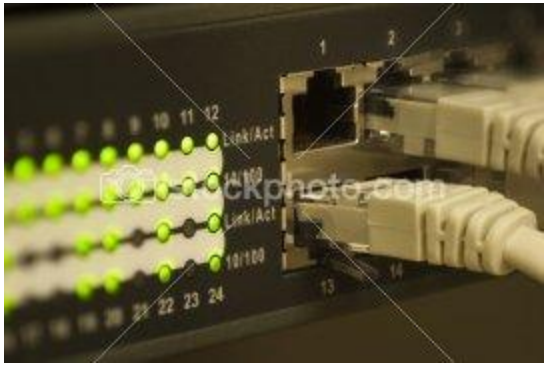
Real World Troubleshooting - Symptom

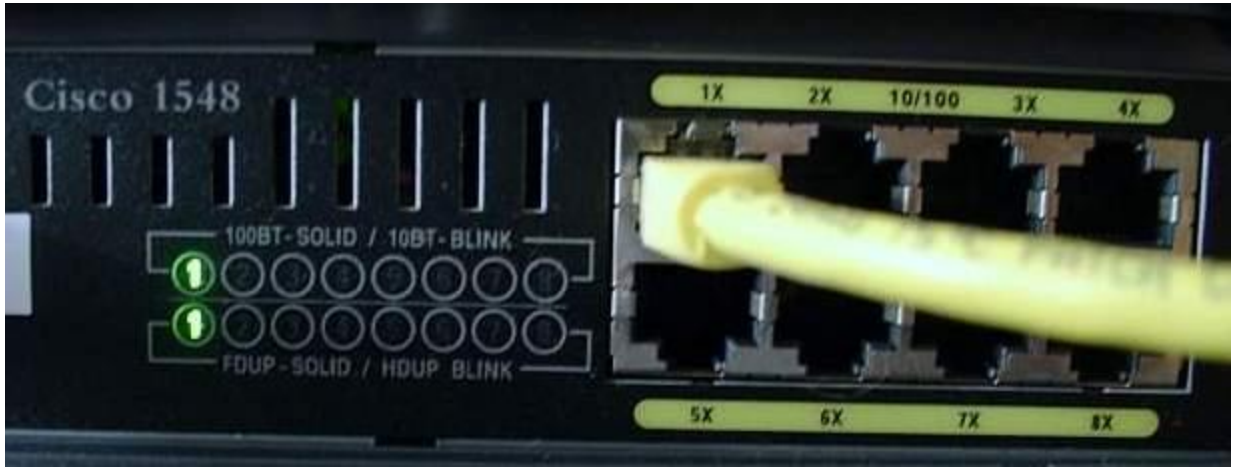


- Hosts connected to switches B, C and D can reach each other and the Internet with no problems.
- However, hosts on X, Y, and Z can either not access hosts on B, C, and D or the Internet, or if they can it is extremely slow.

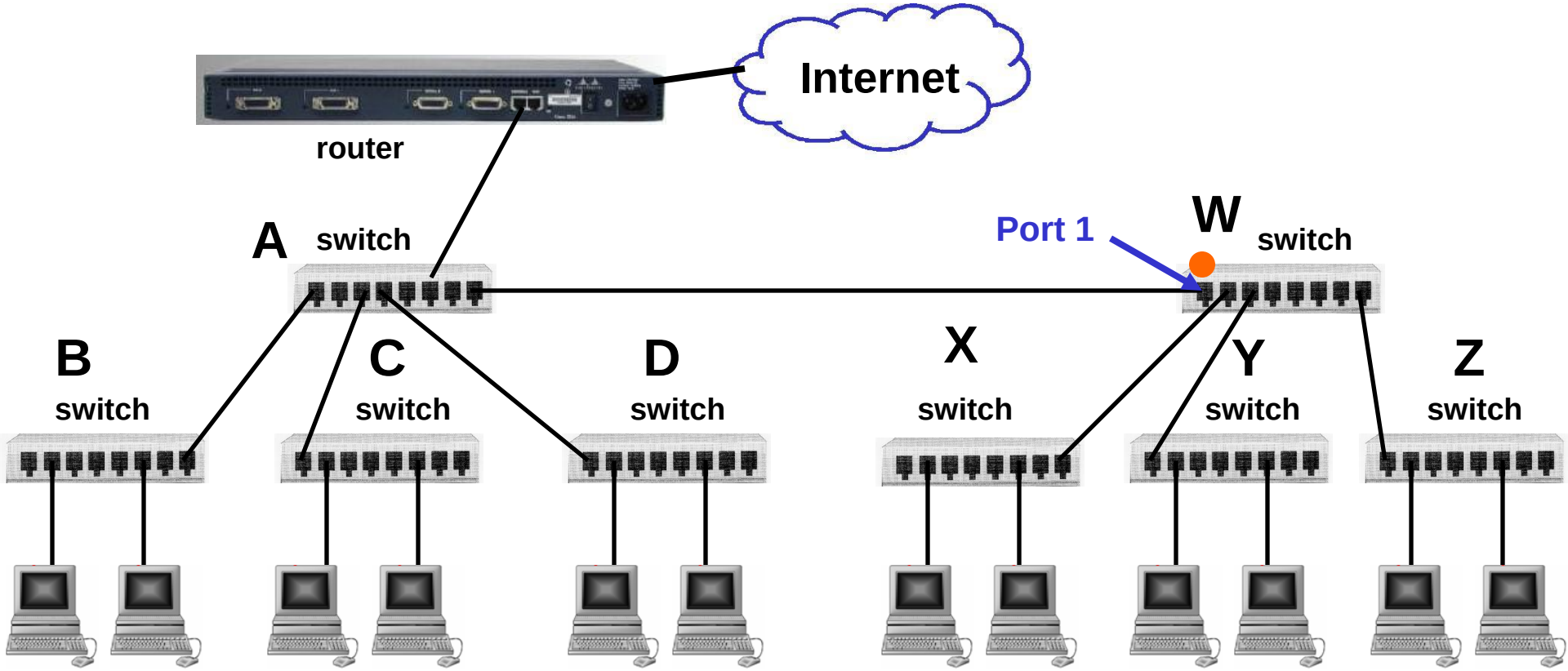
Lights and indicators





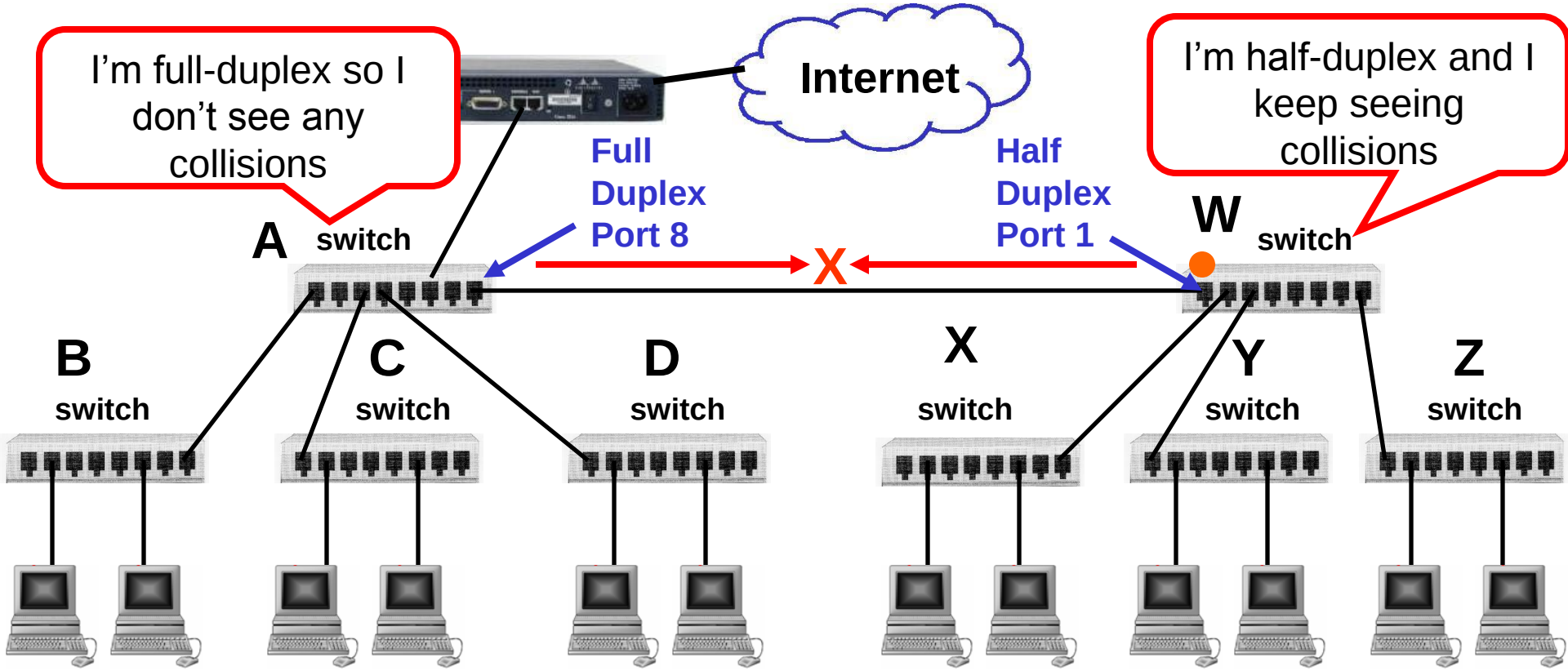


Real World Troubleshooting – Diagnostics



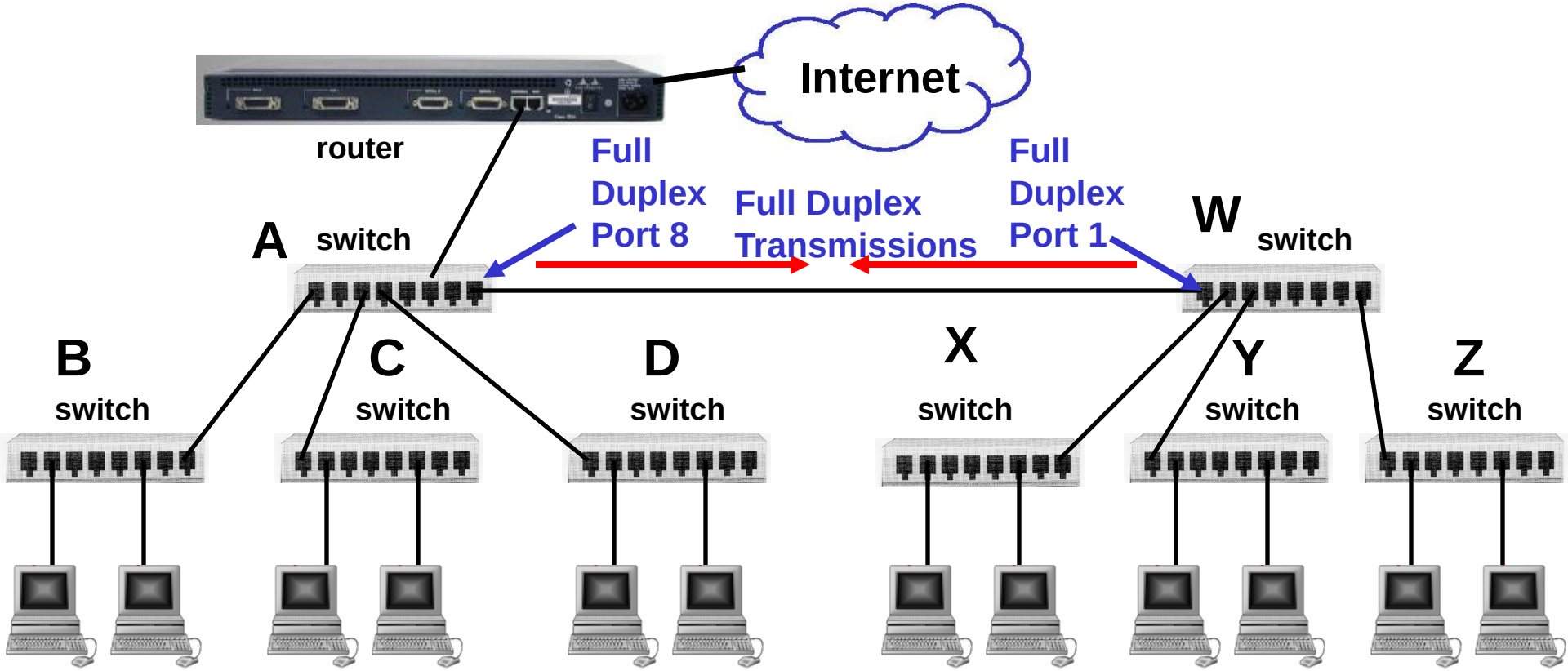
- You notice that a collision light (or looking at some diagnostic output) on Switch W, port 1 is always on indicating a very large number of collisions detected on that port.

Real World Troubleshooting – Problem



- The problem is that
  - Switch A, Port 8 is in Full-duplex mode
  - Switch W, Port 1 is in Half-duplex mode
- Switch A sends whenever it wants to without listening first to see if Switch W is sending.

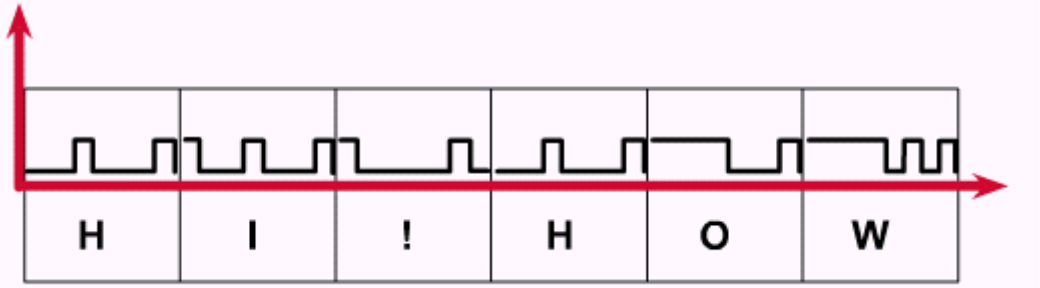
Real World Troubleshooting – Solution



- Configure Switch W, Port 1 to be in full duplex, the same as Switch A, Port A.

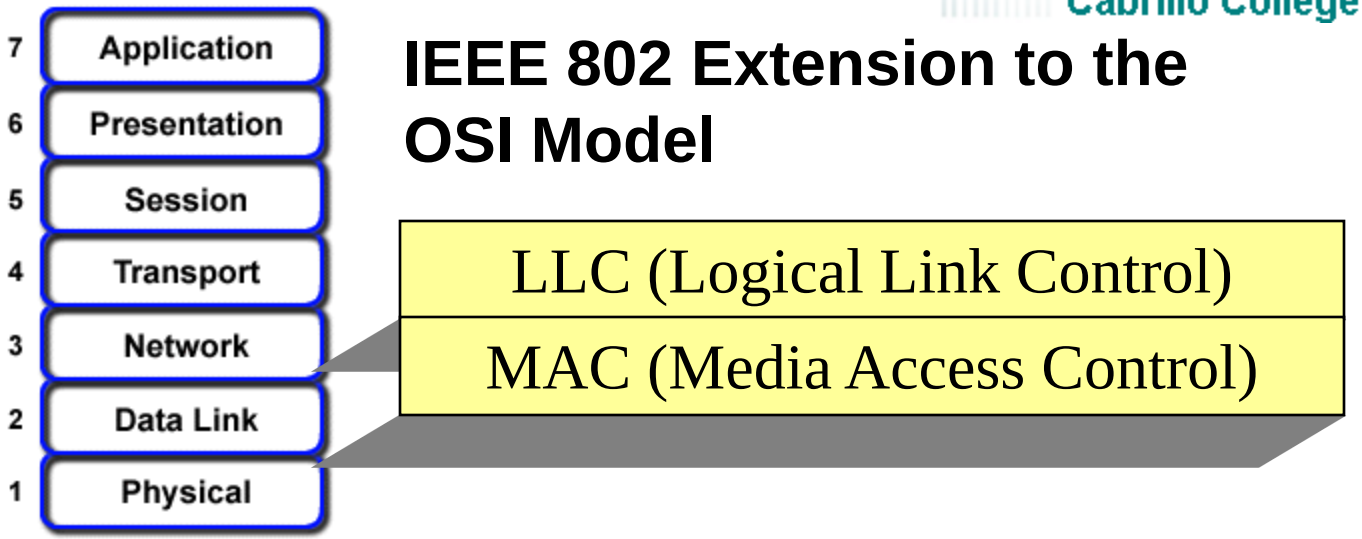
Ethernet and the OSI Model – more detail

Layer 1 Limitations



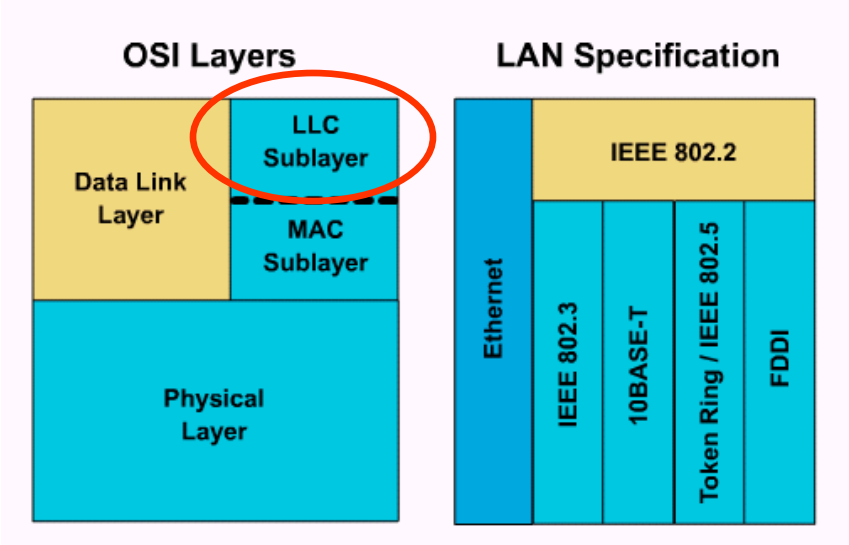
- Layer 1 involves media, signals, bit streams that travel on media, components that put signals on media, and various topologies.
- Layer 1 cannot communicate with the upper-level layers
  - Layer 2 communicates with upper-level layers with ***Logical Link Control (LLC)*.**
- Layer 1 cannot name or identify computers
  - Layer 2 uses an ***addressing*** (or naming) process.
- Layer 1 can only describe streams of bits
  - Layer 2 uses ***framing*** to organize or group the bits.

Data Link Sublayers



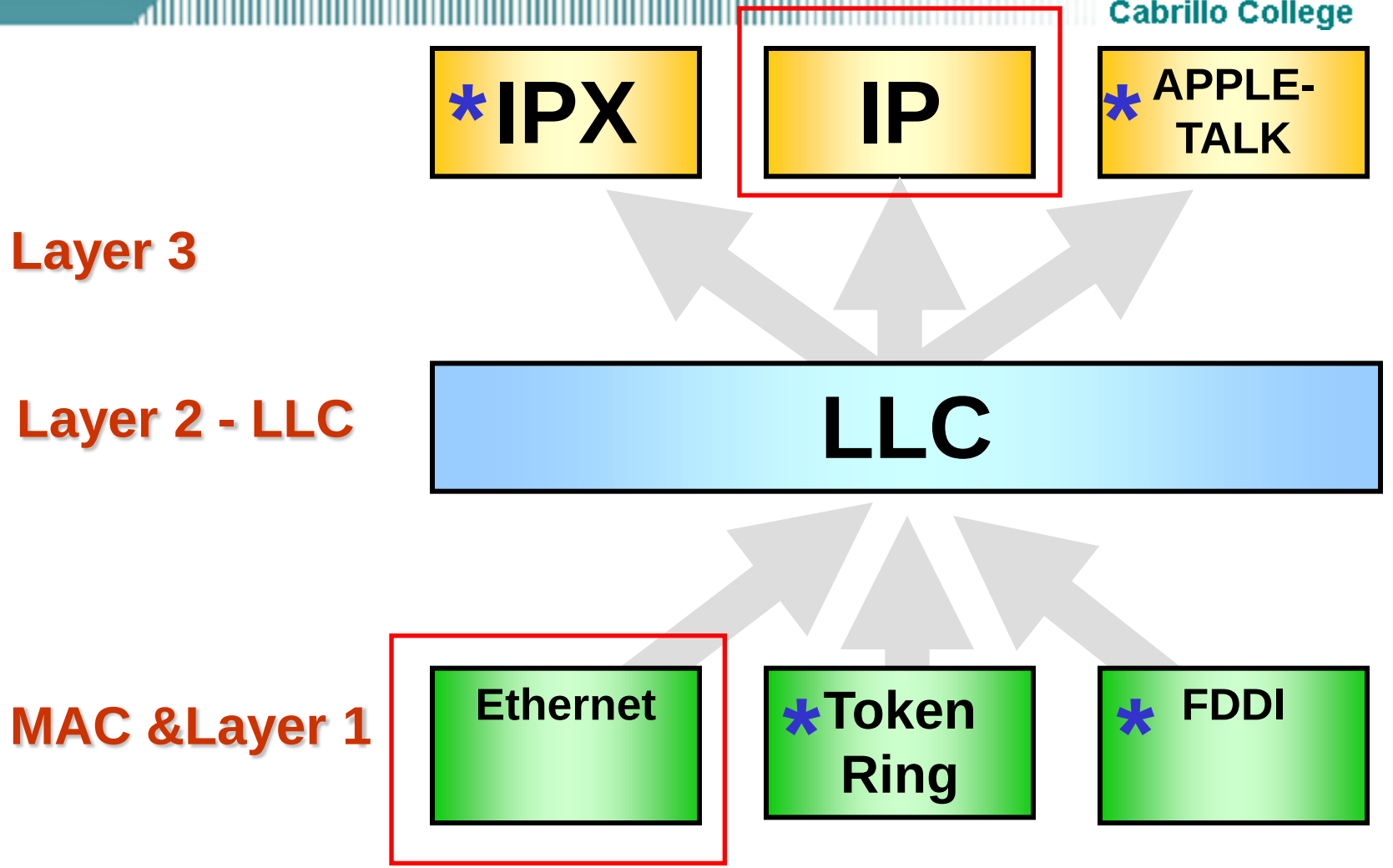
- The Institute of Electrical and Electronic Engineers (IEEE) is a professional organization that defines network standards.
- IEEE 802.3 “Ethernet” is the predominant and best known LAN standards, along with 802.11 (wlan).
- The *IEEE* divides the OSI data link layer into two separate sublayers. Recognized IEEE sublayers are:
  - **Media Access Control (MAC)** (transitions down to media)
  - **Logical Link Control (LLC)** (transitions up to the network layer)

LLC – Logical Link Sublayer



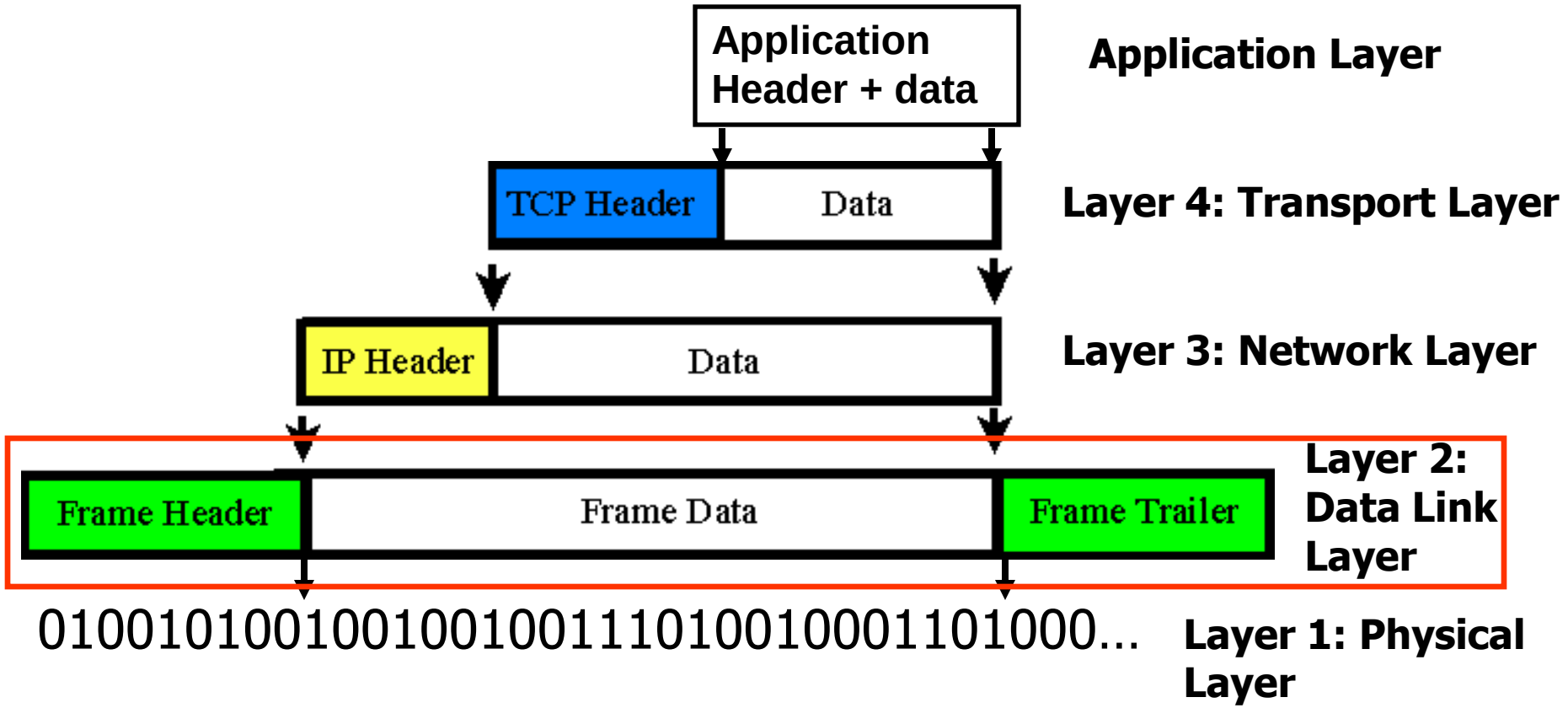
- **Logical Link Control (LLC)** defined in the IEEE 802.2 specification
- Provides versatility in services to network layer protocols that are above it, while communicating effectively with the variety of technologies below it.
- The LLC, as a sublayer, participates in the **encapsulation process**.

802.2 LLC



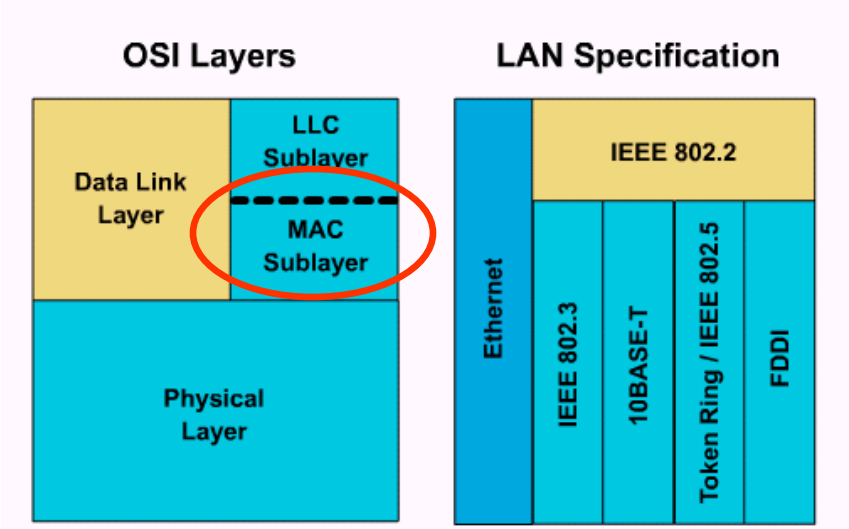
* Legacy technologies

802.2 LLC Data Encapsulation Example



We have been focusing on the Layer 2, Data Link, Ethernet Frame for now.

MAC – Media Access Control Sublayer



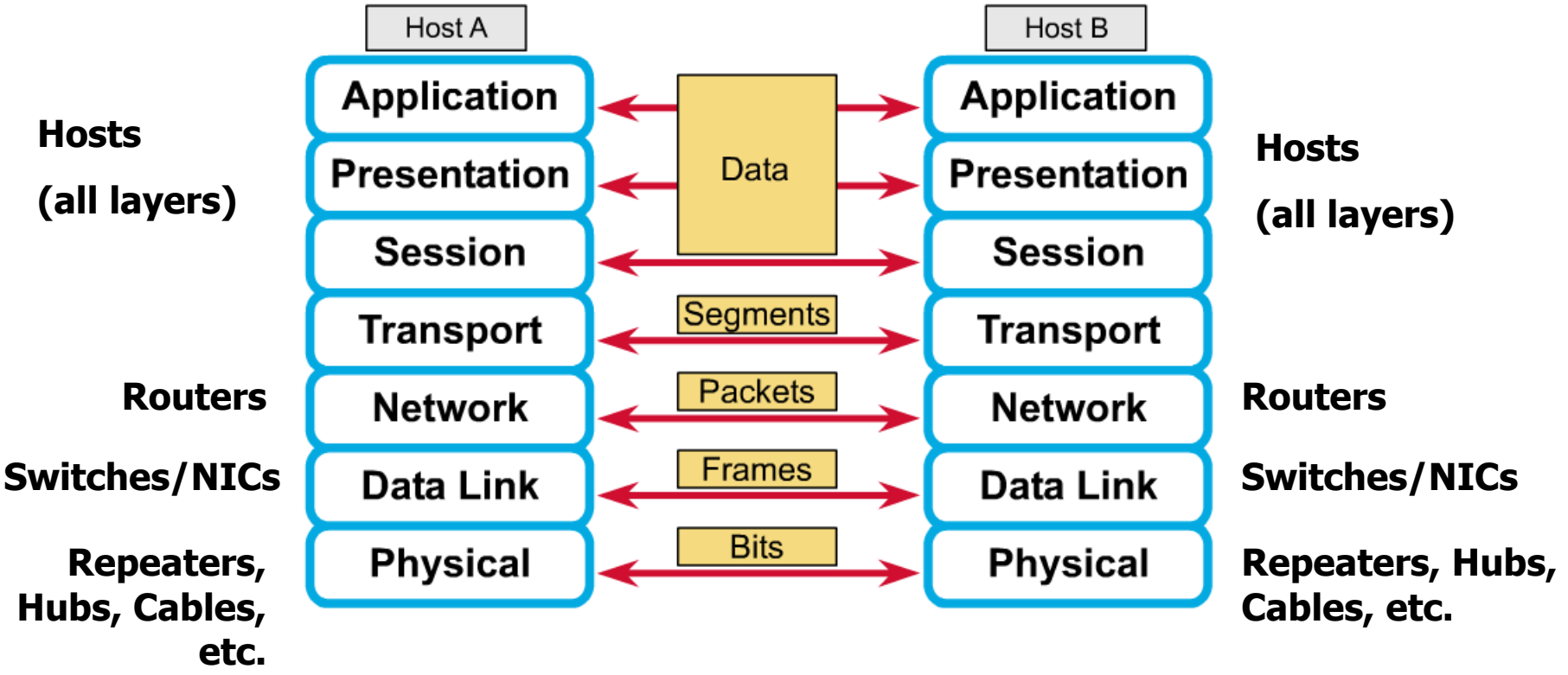
- The **Media Access Control (MAC)** sublayer deals with the protocols that a host follows in order to access the physical media.
- Defined in IEEE 802.3 specification
- Responsible for the actual **framing**
  - Builds the 1s and 0s to hand off to the physical layer.
- Responsible for **media access (CSMA/CD)**

The IEEE Working Groups

802.1	Networking Overview and Architecture
802.2	Logical Link Control
802.3	Ethernet
802.4	Token Bus
802.5	Token Ring
802.6	MANs
802.7	Broadband
802.8	Fiber Optic
802.9	Isochronous LAN
802.11	Wireless LAN

...and more!

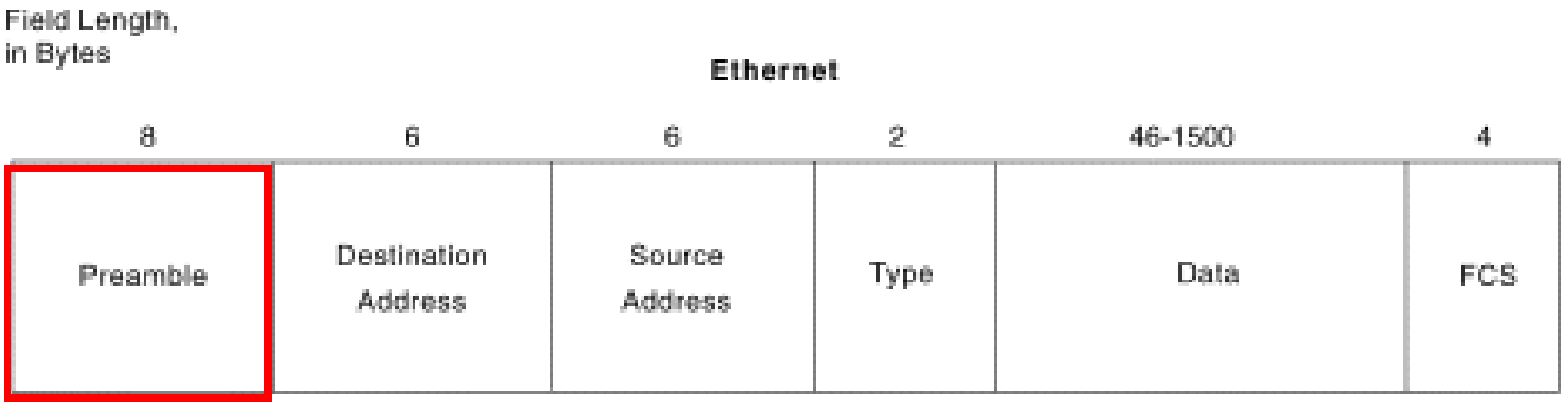
Peer-to-Peer Communications



- Again, we are dealing with just the Data Link (and Physical) layers.

Ethernet Frames – more detail

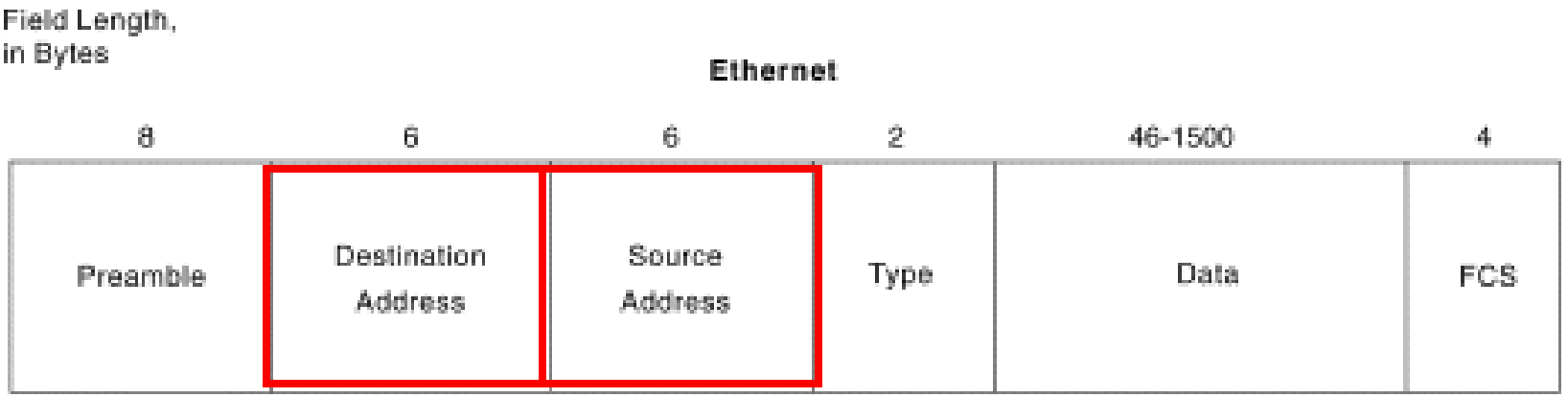
Generic Data Link Frame Format



Preamble or Start Field

- When computers are connected to a physical medium, there must be a way they can grab the attention of other computers to broadcast the message, "Here comes a frame!"
- Various technologies have different ways of doing this process, but all frames, regardless of technology, have a beginning signaling sequence of bytes.
- Depending up frame format: Preamble = 7 bytes, Start or Start of Frame Delimiter (SFD) = 1 byte

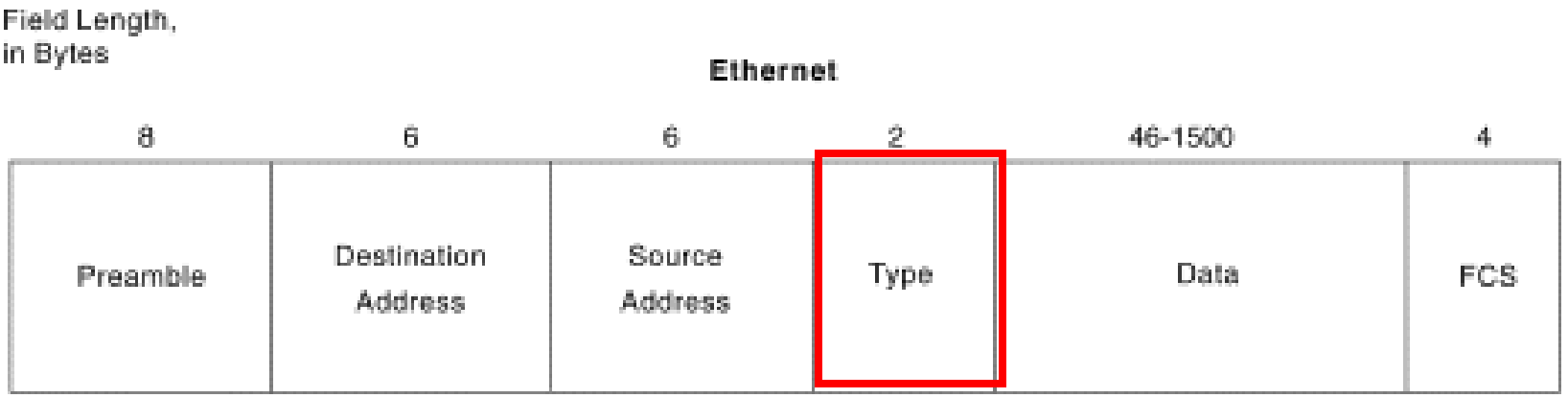
Generic Data Link Frame Format



Address Field

- We saw how IEEE 802.3 uses Destination and Source Addresses.
- By the way: Any idea how a serial data link frame is addressed?
  - **Unicast** address – Single device
  - **Broadcast** address – All devices
  - **Multicast** address – Specific group of devices

Generic Data Link Frame Format



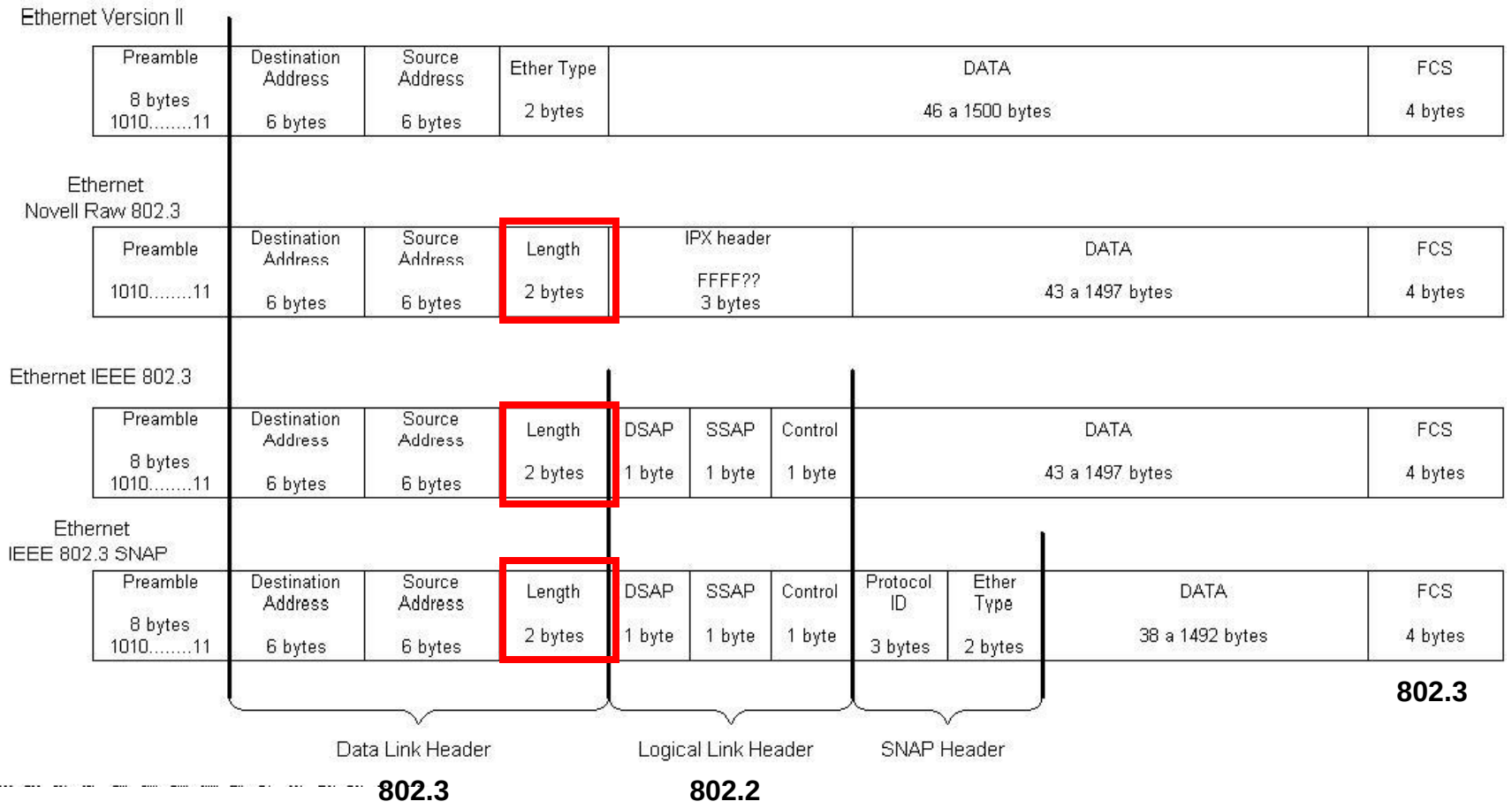
Type Field

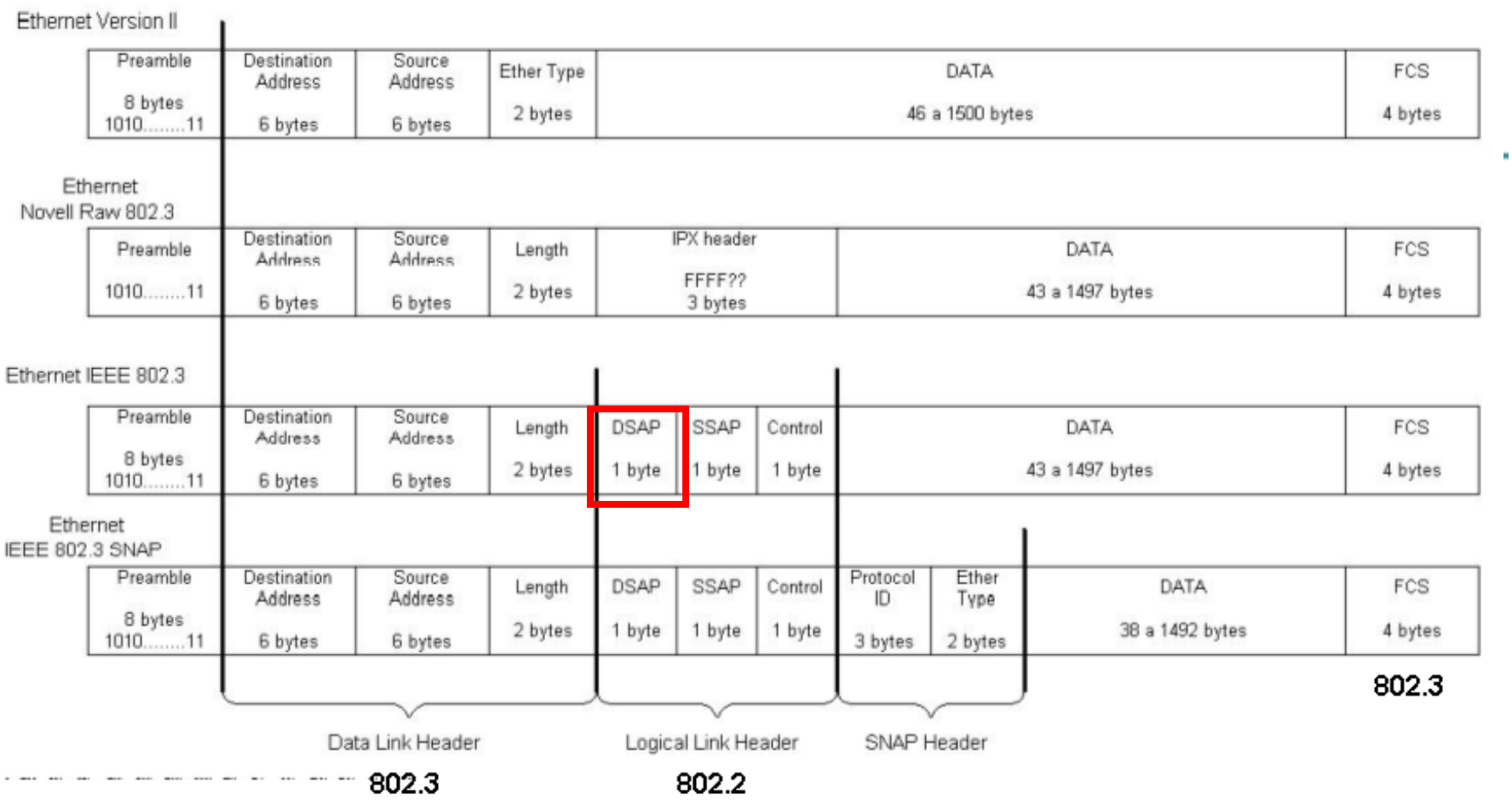
- Usually information indicating the layer 3 protocols in the data field, I.e. IP Packet.
- Type field values of particular note for IEEE 802.3 frames include:
  - 0x0600 XNS (Xerox)
  - **0x0800 IP** (the Internet protocol)
  - 0x8137 Novell NetWare packet formatted for Ethernet II
  - 0x6003 DECNET

“Ethernet” Frame Formats

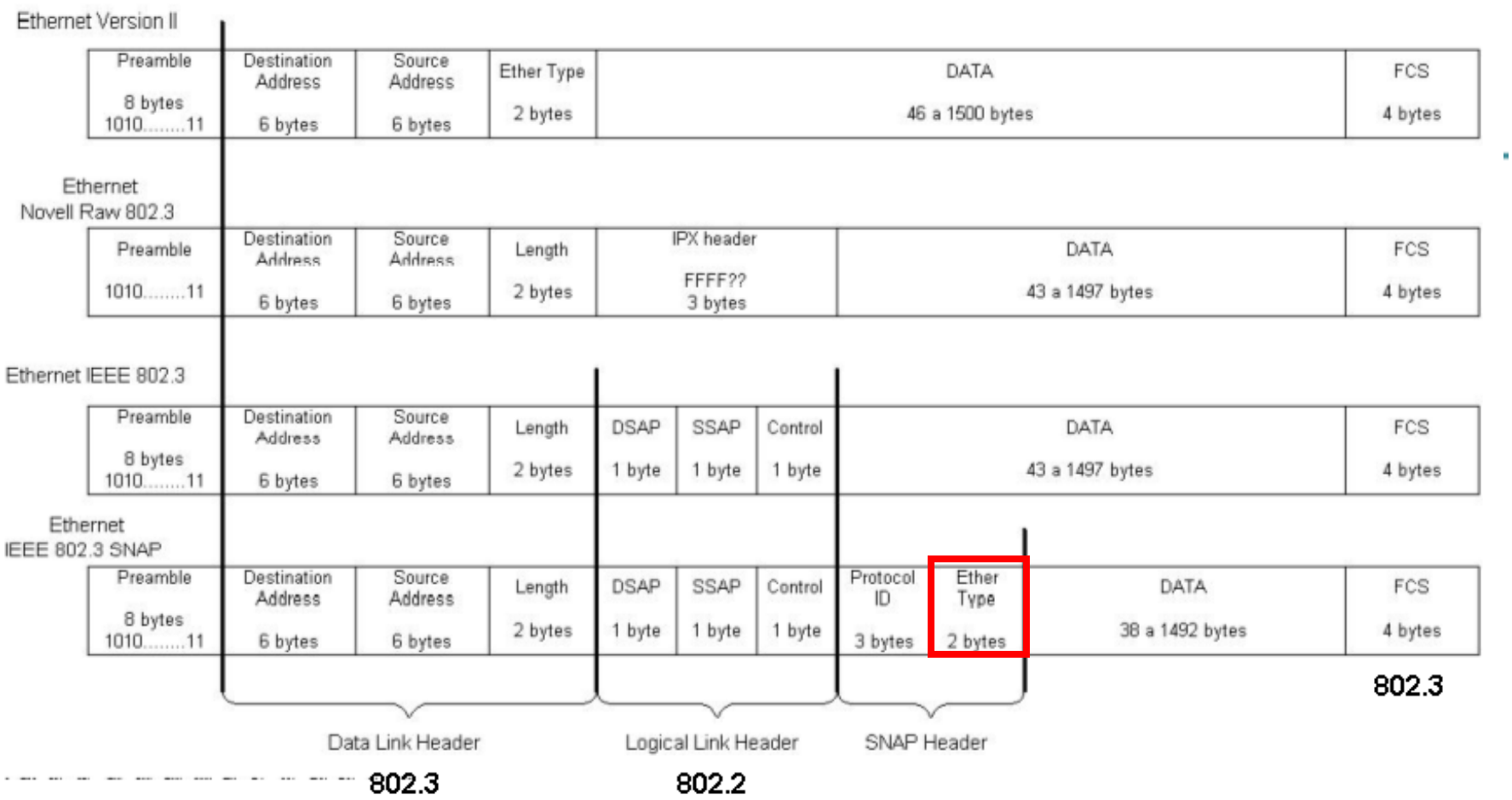
Length Field

- In some frame formats such as 802.3, there is a length field which specifies the exact length of a frame.

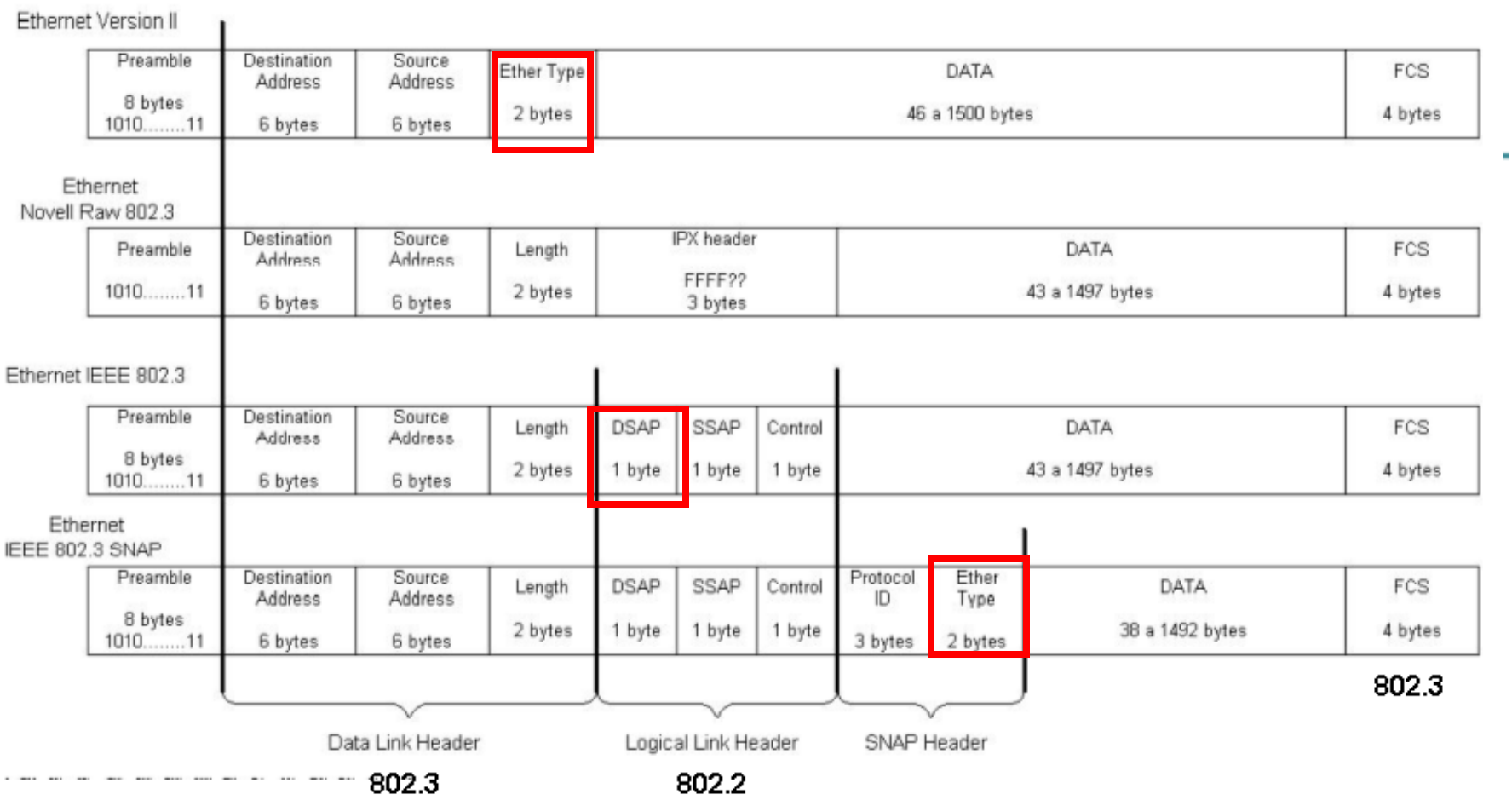




- IEEE 802.3 specification limits the data portion to a maximum of 1500 bytes.
- Designed to hold a Layer 3 IP packet.
- When IEEE created 802.2, it saw the need for a protocol TYPE field that identified what was inside the “data” field.
- IEEE called its 1 byte type field DSAP (Destination Service Access Point).
- Turned out that 1 byte was not long enough to handle all the different number of protocols.

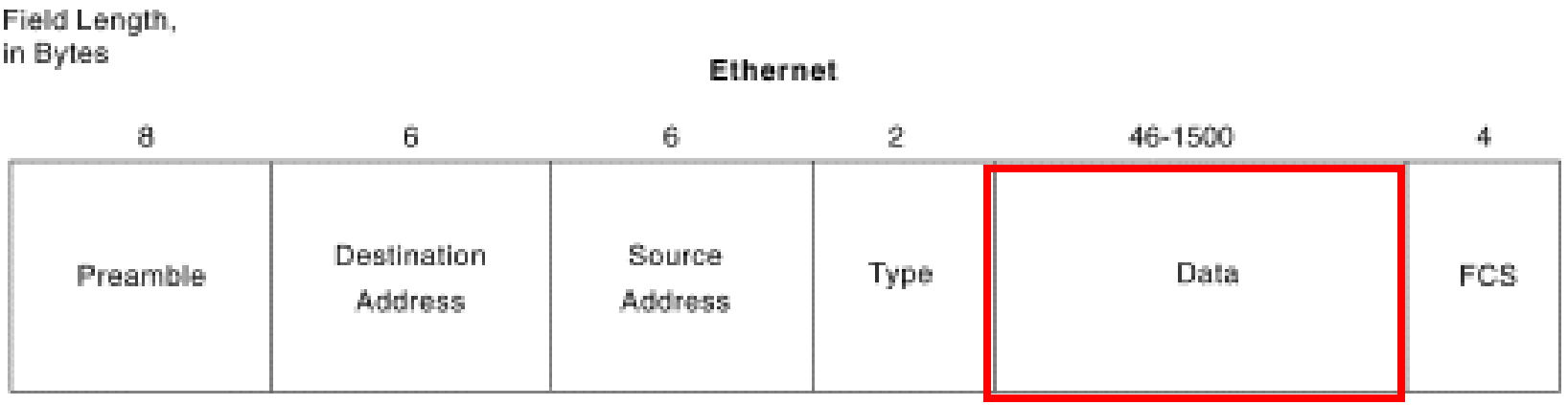


- To accommodate more protocols IEEE added the SNAP (Subnetwork Access Protocol) header.



- The fields of various Ethernet framing that are used for identifying the type of data contained in a frame:
  - **Ethernet II or DIX (DEC, Intel, Xerox) – Most common**
  - IEEE Ethernet (802.3)
  - IEEE 802.3 with SNAP header

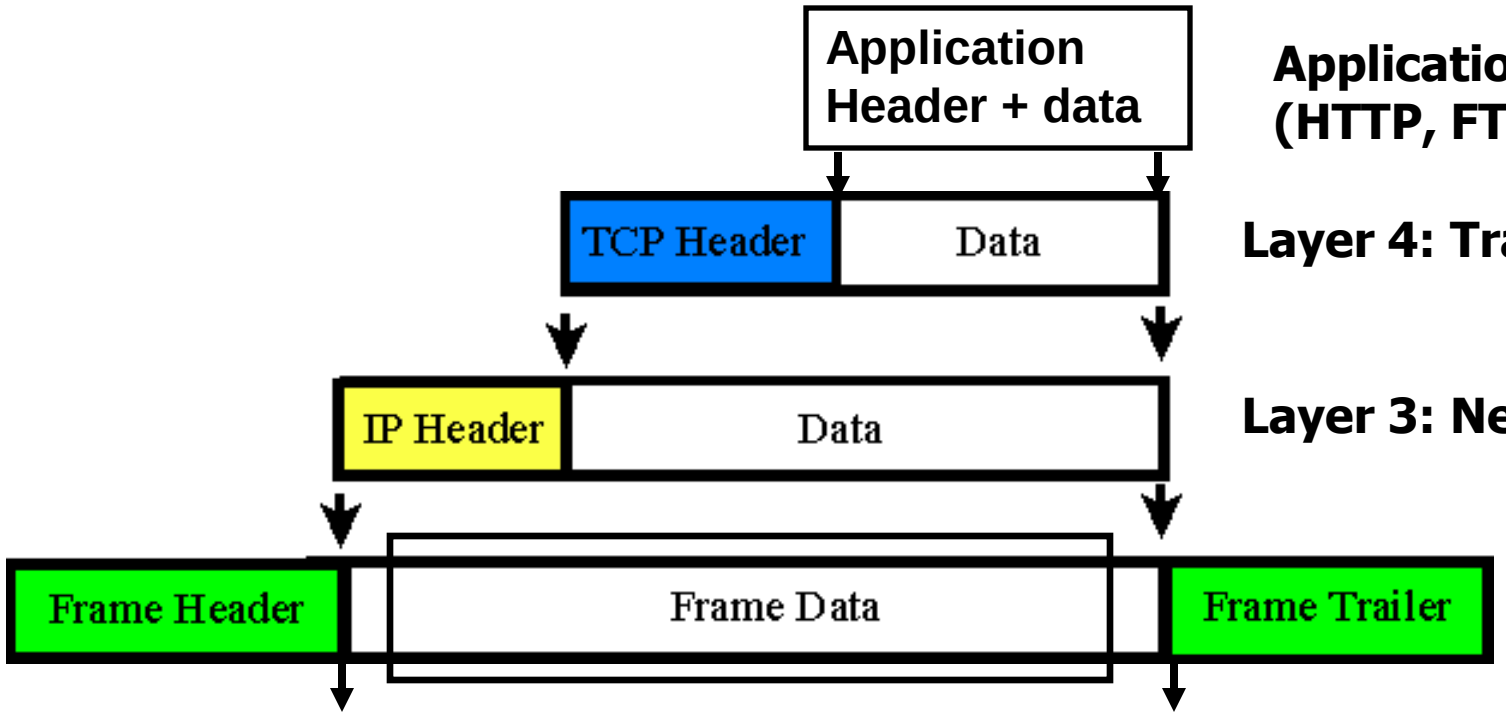
Generic Data Link Frame Format



Data Field

- Included along with this data, you must also send a few other bytes.
- They are called *padding bytes*, and are sometimes added so that the frames have a minimum length for timing purposes.
- LLC bytes are also included with the data field in the IEEE standard frames. (later)

Data Encapsulation Example



Application Layer (HTTP, FTP, etc.)

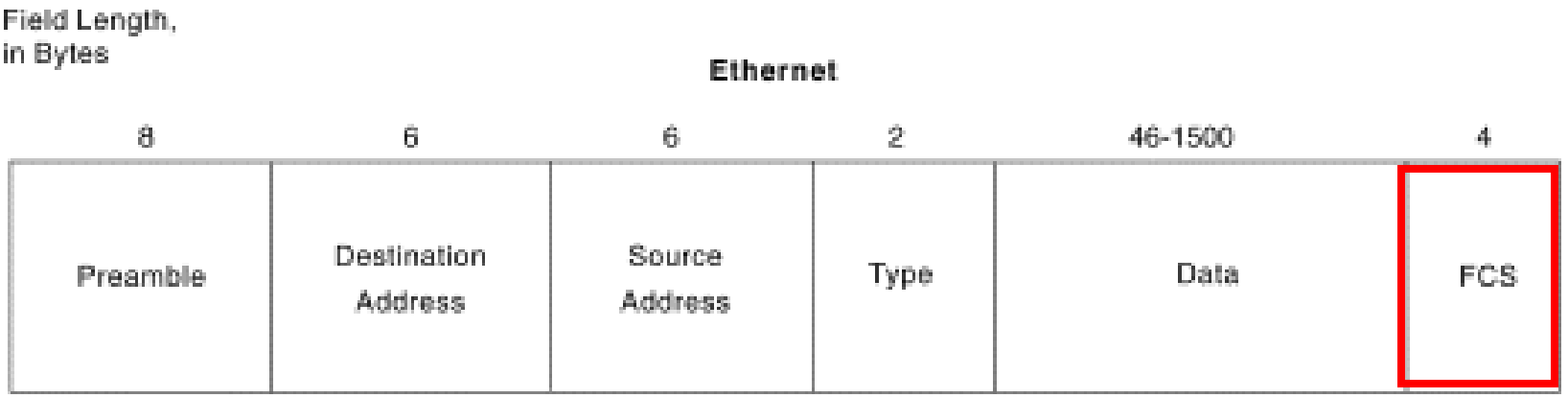
Layer 4: Transport Layer

Layer 3: Network Layer

Layer 2: Data Link Layer

Layer 1: Physical Layer

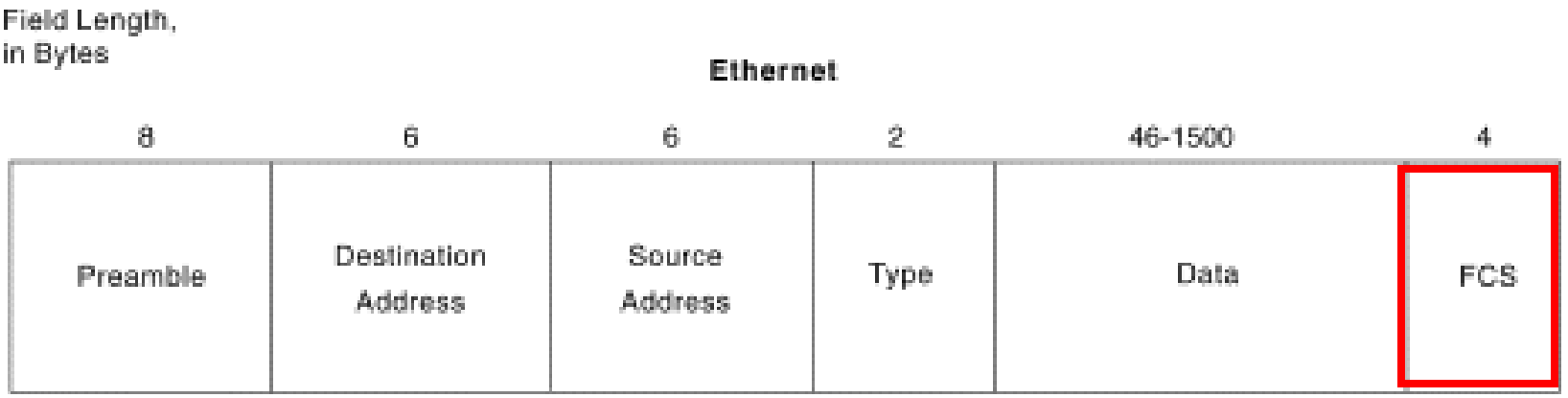
Generic Data Link Frame Format



FCS

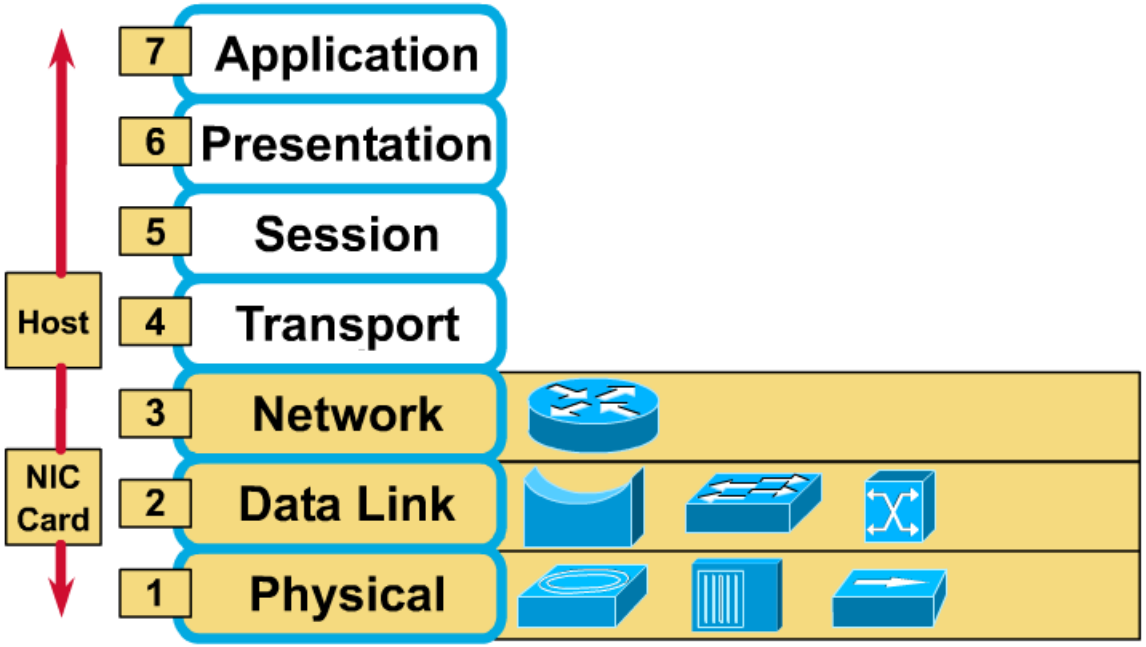
- Used to insure that the data has arrived without corruption.
- More efficient than sending the data twice and comparing the results.
- Necessary to prevent errors.

Three Kinds of FCS

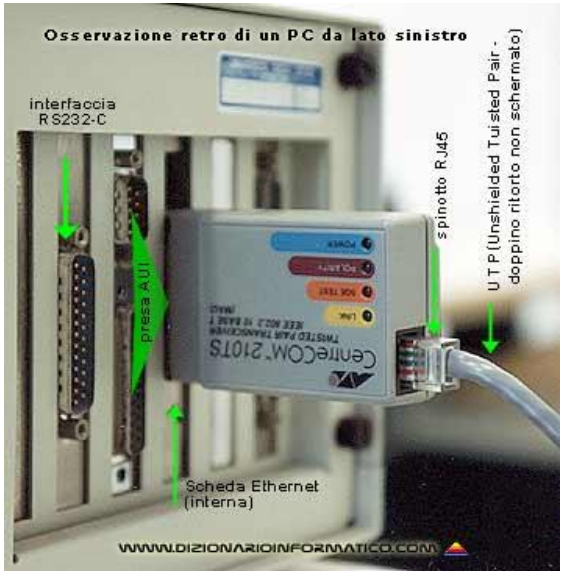


- **Cyclic redundancy check (CRC)**
  - performs polynomial calculations on the data
- **Two-dimensional parity**
  - adds an 8th bit that makes an 8-bit sequence have an odd or even number of binary 1s
- **Internet checksum**
  - adds the numbers to determine a number

Devices and their layers

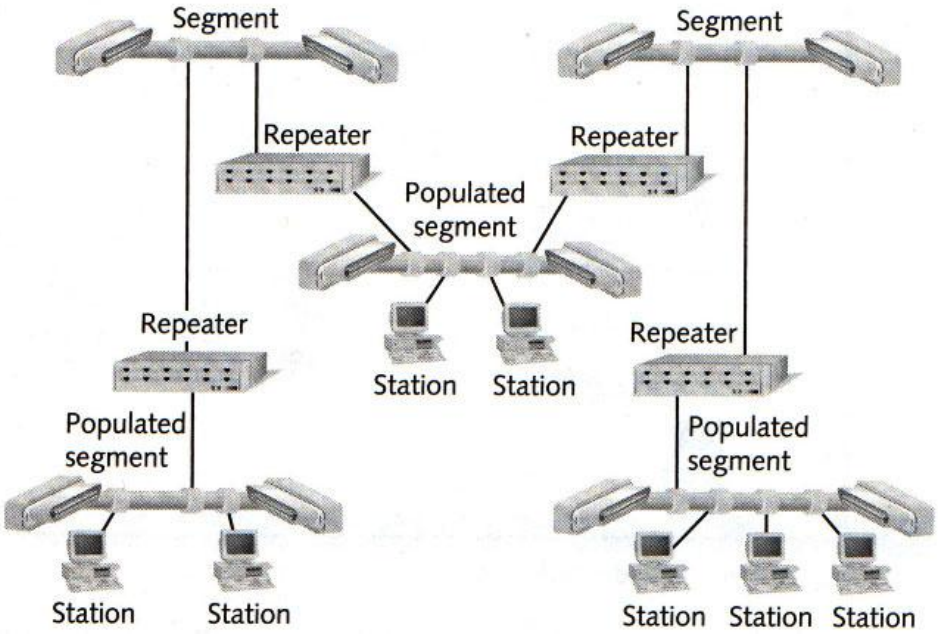


Transceiver



- Hosts and servers operate at Layers 2-7; they perform the encapsulation process.
- **Routers**: Layers 1 through 3, make decisions at layer 3
- **Switches and NICs**: Layers 1 and 2, make decisions at layer 2
- **Hubs and transceivers**: Layer 1, no decisions to make

5-4-3 rule



- "The rule mandates that between any two **nodes** on the network, there can only be a maximum of **five segments**, connected through **four repeaters**, or *concentrators*, and only **three** of the five segments may contain **user connections**." Webopedia.com
- **Note**: This is really no longer an issues with switched networks.

5-4-3 Rule – Webopedia.com

- Ethernet and IEEE 802.3 implement a rule, known as the *5-4-3 rule*, for the number of repeaters and segments on shared access Ethernet backbones in a tree topology. The 5-4-3 rule divides the network into two types of physical segments: populated (user) segments, and unpopulated (link) segments. User segments have users' systems connected to them. Link segments are used to connect the network's repeaters together. The rule mandates that between any two nodes on the network, there can only be a maximum of **five** segments, connected through **four** repeaters, or *concentrators*, and only **three** of the five segments may contain user connections.
- The Ethernet protocol requires that a signal sent out over the LAN reach every part of the network within a specified length of time. The 5-4-3 rule ensures this. Each repeater that a signal goes through adds a small amount of time to the process, so the rule is designed to minimize transmission times of the signals.
- The 5-4-3 rule -- which was created when Ethernet, 10Base5, and 10Base2 were the only types of Ethernet network available -- only applies to shared-access Ethernet backbones. A switched Ethernet network should be exempt from the 5-4-3 rule because each switch has a buffer to temporarily store data and all nodes can access a switched Ethernet LAN simultaneously.

Ethernet Fundamentals Overview: Part 2 (Mod 6)

Cabrillo College

CIS 81 and CST 311

Rick Graziani

Cabrillo College

Spring 2006